SMF & SMAI

L'EXPLOSION DES MATHÉMATIQUES

SMF & SMAI

L'EXPLOSION DES MATHÉMATIQUES

Avant-propos

Nous vivons aujourd'hui une situation pour le moins paradoxale. Les mathématiques sont un instrument irremplaçable de formation à la rigueur et au raisonnement ; elles développent l'intuition, l'imagination, l'esprit critique ; elles sont aussi un langage international, et un élément fort de la culture. Mais elles jouent en outre, par leurs interactions avec les autres sciences, un rôle grandissant dans la conception et l'élaboration des objets de notre vie quotidienne. Or cet état de fait est en général totalement ignoré par la majorité de nos concitoyens, pour qui les mathématiques ont souvent perdu leur sens. Il est parfois de bon ton, y compris dans des postes à responsabilité, de se vanter d'être « nul en maths », ou d'en contester l'utilité.

On peut trouver à ce paradoxe et à cette incompréhension des explications qui tiennent à la spécificité des mathématiques. C'est une discipline qui se nourrit de ses liens avec les autres sciences et avec le monde réel, mais qui également s'enrichit elle-même : les théories ne se démolissent pas, elles se construisent les unes sur les autres. Réciproquement, même si bon nombre de chercheurs en mathématiques sont intéressés avant tout par le côté intellectuel et même esthétique de leur discipline, les applications surgissent parfois de manière inattendue. Ainsi, les applications enrichissent la recherche, mais ne peuvent seules la piloter.

Cet équilibre subtil entre les facteurs de développement interne et externe doit absolument être préservé. Vouloir définir l'activité ou la recherche en mathématiques par ses applications potentielles reviendrait à les faire disparaître. À l'opposé, privilégier l'axiomatisation, l'étude des structures et la dynamique interne de la discipline comme l'ont fait les mathématiques françaises à partir des années 1940, et pendant plusieurs décennies, a conduit à retarder le développement en France des mathématiques dites appliquées, contrairement à ce qui se passait au même moment aux États-Unis et en Union Soviétique. Les facteurs de progrès sont très souvent aux frontières de la discipline.

Aujourd'hui, et nous nous en réjouissons, les mathématiques ont rétabli, et parfois créé, des liens forts avec les autres sciences et avec de nombreux secteurs économiques. La frontière entre mathématiques pures et mathématiques appliquées est devenue floue : les mathématiques les plus fondamentales servent à résoudre des problèmes de plus en plus difficiles. Ainsi, des domaines comme la géométrie algébrique et la théorie des nombres ont trouvé des applications inattendues en théorie du codage et en cryptographie. De même, les liens des mathématiques avec la finance se sont intensifiés pour évaluer, voire créer, des produits financiers de plus en plus complexes, en fonction des besoins et des demandes des acteurs économiques.

Cependant, un travail très important de communication et de sensibilisation reste à faire, pour modifier une image qui, elle, n'a pas suffisamment évolué, et faire découvrir tous les attraits et les atouts du monde des mathématiques et de ses applications. Le but du présent document est de faire connaître les mathématiques sous leurs aspects les plus divers — scientifiques, techniques, culturels, sociologiques; de souligner la diversité et l'universalité d'une discipline qui entretient des liens aussi bien avec la physique, la chimie, l'économie et la biologie qu'avec l'histoire, la musique et la peinture. Les mathématiques sont partout. Sans elles, pas d'ordinateurs, pas de systèmes d'information, pas de téléphonie mobile ; pas d'ateliers de conception pour les constructeurs automobiles et aéronautiques ; pas de systèmes de localisation par satellite, de traitement du signal, de décryptage du génome, de prévisions météo, de cryptographie, de cartes à puce, de robots.

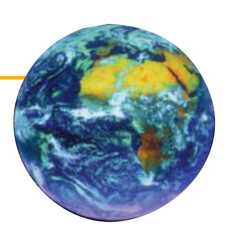
Au-delà de leur rôle de science académique et de formation de base à l'école, les mathématiques sont omniprésentes dans la société d'aujourd'hui. Elles suivent, accompagnent et quelquefois précèdent les développements scientifiques et technologiques actuels, qui font aussi bien appel aux résultats de la recherche fondamentale contemporaine la plus récente qu'ils tirent profit des découvertes accumulées dans le passé. Enfin, les besoins en mathématiques croissent avec l'accélération des mutations et créations technologiques. On ne peut s'en passer, alors qu'on est confronté à la nécessité d'élaborer, de maîtriser, ou d'analyser des systèmes de complexité croissante.

Les États-Unis l'ont bien compris, puisque la NSF (National Science Foundation, l'organisme fédéral chargé de distribuer les crédits pour la recherche universitaire) a décidé depuis l'an 2000 d'augmenter considérablement son soutien financier aux mathématiques. Notre chance est que l'école mathématique française reste une des meilleures au monde, et que la culture mathématique de ses scientifiques et ingénieurs reste de très bon niveau à l'échelle internationale. Le nombre de médailles Fields, équivalent du prix Nobel qui n'existe pas en mathématiques, en témoigne. Récemment, lors du troisième Congrès européen de mathématiques qui s'est tenu à Barcelone en juillet 2000, cinq des dix lauréats primés étaient issus de cette école. Donnons-nous les moyens de garder ce niveau d'excellence.

Mireille Martin-Deschamps
Présidente de la SMF de 1998 à 2001

Patrick Le Tallec
Président de la SMAI de 1999 à 2001

Le temps qu'il fera

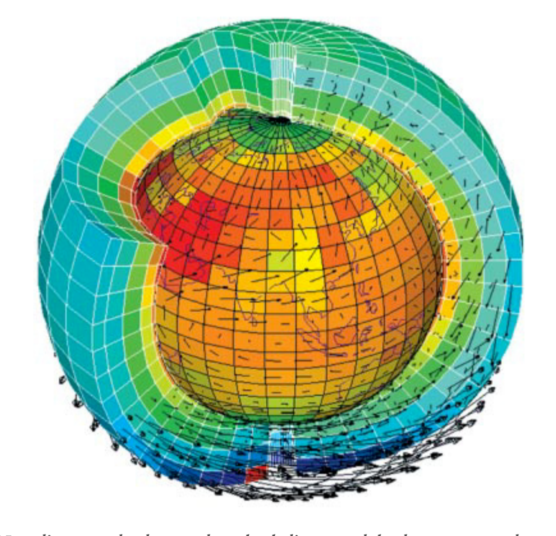


Claude Basdevant

La prévision météorologique ou climatique n'est pas une mince affaire. Elle implique la modélisation de nombreux phénomènes de nature différente et l'intervention de plusieurs sciences, des mathématiques à la biologie, en passant par l'informatique, la physique ou la chimie.

Derrière la charmante présentatrice qui tous les soirs à la télévision nous décrit les prévisions météo pour les jours à venir, il n'y a plus de grenouille et de thermomètre depuis longtemps. Il y a des ordinateurs super-puissants auxquels on a fait absorber un grand nombre de mesures, obtenues principalement par satellites, beaucoup de lois de la mécanique et de la physique, mais aussi beaucoup de mathématiques, parfois très récentes.

Pour que les ordinateurs fournissent des prévisions, il faut élaborer au préalable ce qu'on appelle un modèle numérique de prévision du temps. Schématiquement, un tel modèle de prévision à l'échéance de huit à dix jours représente l'état de l'atmosphère par les valeurs des paramètres météorologiques (vitesse du vent, température, humidité, pression, nuages, etc.) aux centres de « boîtes » d'environ cinquante kilomètres de côté et de quelques dizaines à quelques centaines de mètres de hauteur. Ce découpage imaginaire de toute l'atmosphère en boîtes est inévitable,



Vue d'artiste des boîtes de calcul d'un modèle de prévision du temps ou du climat. (Illustration L. Fairhead LMD/CNRS).

car il est impossible de spécifier les paramètres météorologiques en tous les points de l'atmosphère (ces points sont en nombre infini !). En principe, plus les boîtes sont petites — et donc nombreuses —, plus la description de l'état atmosphérique est précise, et plus les prévisions le seront aussi. Mais en pratique, les boîtes ne font pas moins d'une cinquantaine de kilomètres ; en deçà, la puissance des plus gros ordinateurs ne suffirait pas : il faut bien que le calcul s'achève en temps utile, c'est-à-dire en nettement moins de 24 heures !

Partant de l'état de l'atmosphère supposé connu au début de la période à prévoir, le modèle fait calculer par l'ordinateur son évolution future en utilisant les lois de la dynamique et de la physique. L'évolution dans le temps est calculée pas à pas, par intervalles de quelques minutes. Tel est le principe de la prévision numérique du temps, un principe connu depuis le début du XXe siècle mais qui a attendu les années 1940-1950 et les premiers ordinateurs avant d'être mis en œuvre.

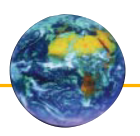
Les mesures météorologiques ne sont pas directement exploitables

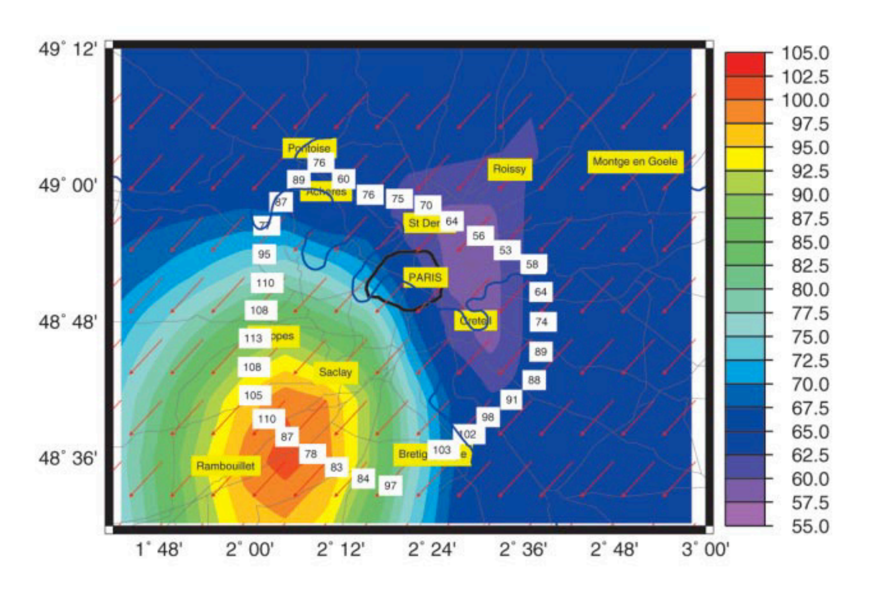
Premier problème dans le schéma idéal de prévision qui vient d'être décrit : savoir construire l'« état initial de l'atmosphère ». Les observations sont loin d'être bien adaptées à cet exercice. Les stations météo au sol sont fort mal réparties sur le globe et fournissent très peu de mesures en altitude. Quant aux satellites, ils sont pour la plupart à défilement, c'est-à-dire qu'ils balayent continûment la Terre. Leurs mesures ne sont donc pas obtenues au même instant en tous points. De plus, les satellites mesurent des quantités intégrées sur toute l'épaisseur de l'atmosphère (il s'agit en général des flux d'énergie reçus dans une certaine gamme de longueurs d'onde) et non pas les grandeurs météorologiques (vent, température, humidité, etc.) qui entrent en jeu dans les équations des modèles.

On dispose donc d'une masse de données disparates, mal distribuées à la surface du globe, étalées sur 24 heures, avec lesquelles il faut « initialiser » une prévision, c'est-à-dire construire un état météorologique initial dont le modèle simulera l'évolution. Or grâce aux travaux sur l'*optimisation dynamique*, domaine auquel ont beaucoup contribué le chercheur russe Lev Pontriaguine (1908-1988) et l'école mathématique française, on a pu mettre au point, dans les années 1980, des méthodes dites d'« assimilation variationnelle » qui permettent de reconstruire de façon optimale l'état initial. L'idée sous-jacente à ces méthodes, opérationnelles depuis l'année 2000 à Météo-France, est d'obliger en quelque sorte la trajectoire du modèle numérique à passer « près » des données observées pendant les 24 heures précédentes. L'assimilation variationnelle n'est d'ailleurs pas la seule technique mathématique moderne qui a bouleversé le traitement des observations : l'utilisation des réseaux neuromimétiques ou des ondelettes, inventés depuis moins de vingt ans, a donné lieu à des gains spectaculaires en efficacité, précision et rapidité dans le traitement des données fournies par les satellites.

Quand l'analyse numérique entre en action…

Une fois connu l'état atmosphérique initial dont a besoin le modèle numérique de prévision, reste à écrire le programme informatique capable de calculer le temps futur à partir de cet état initial et des lois de la physique. Celles-ci reposent sur une description continue de l'espace et du temps ; mais notre modèle numérique, lui, ne connaît qu'un nombre, certes grand, mais fini, de boîtes ; de même, les intervalles de temps entre deux états calculés sont de plusieurs minutes — on dit que le problème a été « discrétisé ». Passer des équations continues à des schémas numériques pour le modèle discrétisé, tout en gardant la meilleure précision possible, tel est le domaine de l'analyse numérique, une branche des mathématiques qui a explosé depuis l'ar-





Panache d'ozone sur la région parisienne le 7 août 1998 à 16 heures et 300 m d'altitude. Codées en couleurs, les concentrations simulées par le modèle numérique CHIMERE du LMD/IPSL ; en incrustation, les mesures par avion (Illustration MERLIN de Météo-France).

rivée des ordinateurs. L'analyse numérique a pour but de savoir résoudre des équations et mener les calculs jusqu'au bout, c'est-à-dire jusqu'à l'obtention de valeurs numériques précises, en investissant le moins de temps et d'efforts possible. Elle est indispensable pour que simulation ne soit pas synonyme de simulacre et pour évaluer l'incertitude des prévisions. Par exemple, des progrès très importants ont été obtenus récemment concernant les méthodes permettant de simuler le déplacement des espèces chimiques ou des particules dans la turbulence atmosphérique. Ces avancées ont significativement amélioré l'étude et la prévision de la pollution de l'air.

Peut-on prédire le temps longtemps à l'avance ? Non, indique la théorie des systèmes dynamiques

On a évoqué jusqu'ici la prévision du temps à courte échéance, de huit à dix jours. Mais pourquoi ne fait-on pas des prévisions à plus longue échéance ? Le météorologue américain Edward N. Lorenz, dans un célèbre article de 1963, a montré que c'était probablement sans espoir. L'atmosphère est un système chaotique, c'est-à-dire que toute erreur sur l'état météorologique initial, aussi petite soit-elle, s'amplifie rapidement au cours du temps ; si rapidement qu'une prévision à l'échéance d'une dizaine de jours perd toute sa pertinence. Néanmoins, cela ne veut pas dire que l'on ne peut pas prévoir le climat — c'est-à-dire faire une prévision de type statistique plutôt que déterministe, s'intéresser à la moyenne des températures ou des précipitations sur une période, plutôt qu'au temps précis qu'il fera sur la Bretagne tel jour du mois de juillet. L'enjeu est d'importance : notre climat futur est menacé par les rejets de gaz dus aux activités humaines et il faut prévoir l'effet à long terme de ces perturbations. C'est la théorie des *systèmes dynamiques* qui donne des outils pour justifier cette modélisation du climat. Ce domaine, pour lequel le mathématicien Henri Poincaré, au début du XXe siècle, fut un grand précurseur, a connu des progrès très importants dans les vingt dernières années. La théorie des systèmes dynamiques permet par exemple de dégager ce que les mathématiciens appellent des attracteurs, ou des régimes de temps pour les météorologues. Elle permet aussi de savoir quels sont les régimes de temps les plus prévisibles et ceux qui sont les plus instables. Dans les situations d'instabilité, un bon outil serait la modélisation probabiliste du climat, c'est-à-dire la conception de modèles prenant explicite-

ment en compte le caractère aléatoire de la prévision. Encore peu développées, les modélisations de ce type doivent s'appuyer sur des outils très récents de la théorie des *équations aux dérivées partielles stochastiques* et des statistiques.

Des prévisions météorologiques aux prévisions climatiques

Les modèles numériques de prévision du climat ressemblent comme des frères aux modèles de prévision du temps, à deux différences essentielles près. Pour des raisons de temps de calcul, leurs « boîtes » sont plus grandes (200 à 300 km de côté) ; les temps simulés allant de quelques mois à des centaines voire des milliers d'années, il est impossible d'être plus précis. Mais la différence importante tient au fait que les variations climatiques ont lieu à de longues échelles de temps, et qu'il n'est alors plus possible de négliger les interactions entre l'atmosphère, l'océan, les glaces de mer, voire la biosphère. C'est pourquoi un modèle de climat doit combiner un modèle d'atmosphère, un modèle d'océan, un modèle de glaces de mer, un modèle de biosphère. Au-delà de la complexité informatique d'une telle construction, se posent de délicats problèmes mathématiques sur la bonne manière de coupler ces domaines et sur la spécification des conditions aux interfaces atmosphère-océan, océan-glaces, etc. Et pour que le calcul dans les « grandes boîtes » reste significatif, il faut évaluer l'effet statistique, à l'échelle de cette boîte, de processus qui se produisent à des échelles beaucoup plus petites (par exemple : quel est l'effet statistique, sur le bilan d'énergie d'une boîte de 300 km de côté, des petits cumulus de quelques km de diamètre qui s'y développent ?). Il reste, dans toutes ces questions, encore beaucoup de matière à développements mathématiques.

Claude Basdevant
Laboratoire de météorologie dynamique,
École normale supérieure, Paris et
Laboratoire Analyse, géométrie et applications,
Université Paris-Nord.

Quelques références :

- *La Météorologie, n° 30*, numéro spécial sur la prévision météorologique numérique (2000).
- M. Rochas, et J.-P. Javelle, *La Météorologie - La prévision numérique du temps et du climat* (collection « Comprendre », Syros, 1993).
- R. Temam et S. Wang, « Mathematical Problems in Meteorology and Oceanography », *Bull. Amer. Meteor. Soc., 81*, pp. 319-321 (2000).

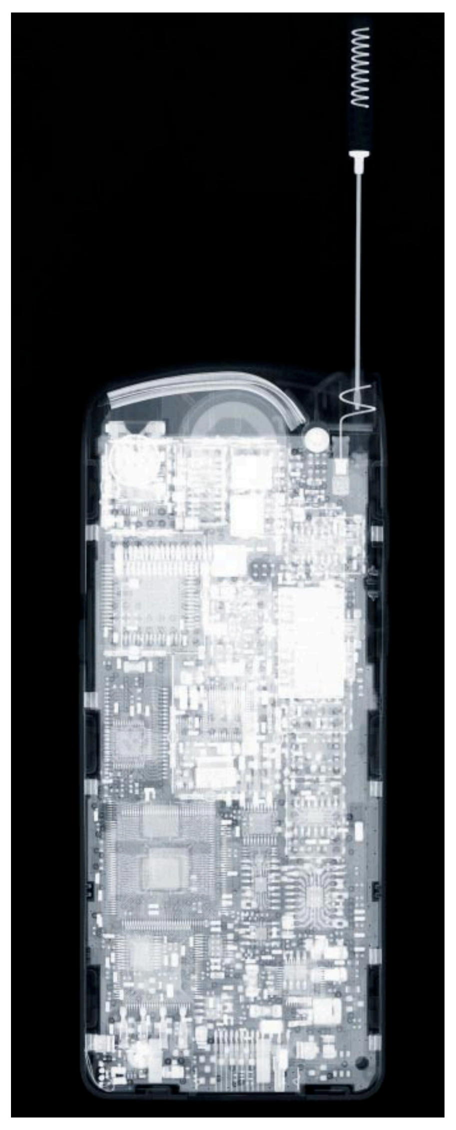
Les dessous du téléphone portable



Daniel Krob

Le téléphone mobile est maintenant un objet relativement banal. Qui n'a jamais vu un portable ou téléphoné avec ? Mais rares sont ceux qui ont une pensée pour la science et la technologie mises en jeu.

Le téléphone mobile est aujourd'hui d'un usage très courant dans beaucoup de pays. Il n'y a pas si longtemps, la situation était bien différente. En 1985, existaient un grand nombre de systèmes de téléphonie sans fil, conçus, développés et commercialisés par les grands opérateurs nationaux historiques; mais ils étaient mutuellement incompatibles. Différant par leurs caractéristiques techniques, ces systèmes ne permettaient pas de communiquer d'un réseau à l'autre. Pour les rendre compatibles, il fallait donc se mettre d'accord sur tout un ensemble de spécifications techniques, c'est-à-dire sur une norme commune. Cela a débuté au cours des cinq années suivantes, quand a émergé en Europe la norme GSM (*Global System for Mobile communications*), à la suite d'une initiative de France Télécom et de Deutsche Telekom, les deux opérateurs téléphoniques français et allemand de l'époque. Les premiers systèmes commerciaux fondés sur cette norme ont alors vu le jour au début des années 1990. Mais ce n'est finalement que vers le milieu, pour ne pas dire la



Une radiographie d'un téléphone mobile. L'électronique de cet appareil semble compliquée, mais elle ne laisse pas entrevoir les travaux de nature mathématique qui ont été nécessaires pour mettre au point la téléphonie mobile. (Cliché Stock Image)



fin, de cette même décennie que le GSM s'est vraiment imposé comme le seul réel standard international de téléphonie mobile. Le développement actuel des réseaux mobiles de troisième génération est d'ailleurs un excellent témoin de l'importance prise par le GSM, dans la mesure où la norme sous-jacente à cette troisième génération, l'UMTS (*Universal Mobile Telecommunications System*), constitue une extension naturelle de la norme GSM.

La norme GSM cache une grande complexité scientifique et technologique

L'utilisateur a rarement conscience que, derrière les réseaux radio-mobiles, se cache une grande complexité scientifique et technologique. Par exemple, la norme GSM représente plus de 5 000 pages de spécifications techniques, difficiles à lire même pour le spécialiste ! Et le GSM est loin d'être figé : d'énormes efforts de recherche et développement sont investis, tant par les grandes sociétés d'ingénierie radio-téléphonique que par les laboratoires universitaires, pour améliorer sans cesse la qualité et l'efficacité des réseaux de téléphonie mobile.

La norme GSM repose sur un ensemble de techniques élaborées provenant tant des télécommunications classiques que de l'informatique, des mathématiques et du traitement du signal. En particulier, les mathématiques et l'algorithmique jouent un rôle fondamental dans la conception et le bon fonctionnement des mécanismes internes des réseaux radio-mobiles. Les mathématiques fournissent le substrat théorique sur lequel s'appuient presque toutes les étapes fondamentales de traitement de l'information nécessaires à la gestion d'une communication téléphonique à partir d'un portable. L'algorithmique, elle, permet de transformer ces résultats fonda-



Une antenne relais pour la téléphonie mobile GSM, en campagne, sur exploitation agricole. (Cliché REA)



mentaux en protocoles effectifs et efficaces, pouvant être mis en œuvre concrètement au sein d'un réseau radio-mobile.

Des algorithmes pour numériser l'information, la découper en paquets, la crypter, etc.

Pour illustrer l'impact de ces deux disciplines en téléphonie mobile, regardons un peu plus en détail la manière dont une communication téléphonique est gérée lorsqu'un utilisateur compose un numéro sur son appareil. Tout d'abord, toutes les données transmises au sein d'un réseau radio-mobile sont uniquement numériques : elles sont en effet constituées de « paquets », c'est-à-dire de suites de 0 et de 1 de longueur fixe, émis tous les quarts de seconde, qui contiennent l'ensemble des informations (parole, identification du portable, qualité de réception telle que la mesure le mobile, etc.) liées à une communication téléphonique donnée. Outre la gestion de la mobilité des utilisateurs, la grande différence entre la téléphonie mobile et la téléphonie fixe classique réside bien entendu dans le fait que les paquets d'information numérique sont transmis par ondes hertziennes et non par câbles ; cela a nécessité la mise au point d'un ensemble de techniques algorithmiques et mathématiques très spécifiques. Celles-ci font intervenir à la fois de l'algorithmique répartie, de l'optimisation combinatoire, du traitement numérique du signal, de la géométrie algorithmique ou du codage correcteur d'erreurs, pour ne citer que quelques domaines parmi beaucoup d'autres.

Les paquets d'information ne sont en effet pas transmis de manière brute. Pour assurer la confidentialité des communications, chaque paquet est crypté à l'aide d'un protocole cryptographique spécifié par la norme et utilisant des clefs secrètes propres à chaque opérateur (et l'on sait que les méthodes cryptographiques reposent sur des techniques et concepts algébriques ou géométriques souvent très élaborés). La gestion de la transmission hertzienne proprement dite nécessite elle-même un traitement préalable de chaque paquet d'information. Le canal hertzien est en effet soumis à plusieurs types de perturbations qui affectent les signaux émis par un portable. Par exemple, les absorptions et réflexions des ondes hertziennes par les bâtiments entraînent une atténuation et un déphasage de chaque signal émis par un portable. De même, chaque signal engendre de nombreux échos, dont il faut tenir compte. Aussi, une partie de chaque paquet d'information est spécialement dévolue à la récupération du signal d'origine au sein de la mer d'échos dans laquelle il est noyé.

Ces problèmes ont bien entendu été étudiés depuis longtemps, tant au niveau théorique que pratique. Les contraintes d'ingénierie propres aux réseaux radio-mobiles ont néanmoins nécessité de développer et d'adapter une partie importante de l'appareil mathématique classiquement utilisé dans ces contextes.

De la théorie des graphes pour allouer convenablement les fréquences

L'apport de l'algorithmique et des mathématiques ne se limite pas à la chaîne de traitement de l'information numérique que nous venons (très rapidement) d'esquisser. Les techniques algorithmiques sont en particulier fon-

damentales pour gérer efficacement les fréquences radio dont dispose chaque opérateur. Les pouvoirs publics louent — relativement cher — à chaque opérateur la bande de fréquence qu'il peut utiliser ; cependant, seul un petit nombre, de l'ordre de 300, de fréquences est réellement utilisable au sein de cette bande. Deux communications réalisées en même temps par deux portables différents, mais géographiquement proches, ne peuvent être acheminées sur des fréquences voisines sous peine d'interférences affectant la qualité des transmissions. Il est donc nécessaire de savoir répartir de façon optimale les fréquences disponibles parmi tous les utilisateurs — qui sont bien plus nombreux que les fréquences. On peut démontrer qu'un être humain n'est pas capable de résoudre exactement ce type de problème en un temps raisonnable. Les méthodes algorithmiques, fondées sur des modèles mathématiques tels que la théorie des graphes, ont ici été déterminantes pour réaliser des logiciels de planification qui permettent effectivement de résoudre — de manière approchée — ces problèmes d'allocation de fréquences. Tous ces problèmes ont une grande importance du point de vue industriel, et font encore l'objet de recherches très actives.

Daniel Krob
Directeur de recherches au CNRS et directeur du LIAFA (Laboratoire d'informatique algorithmique : fondements et applications), Université Paris 7 et CNRS

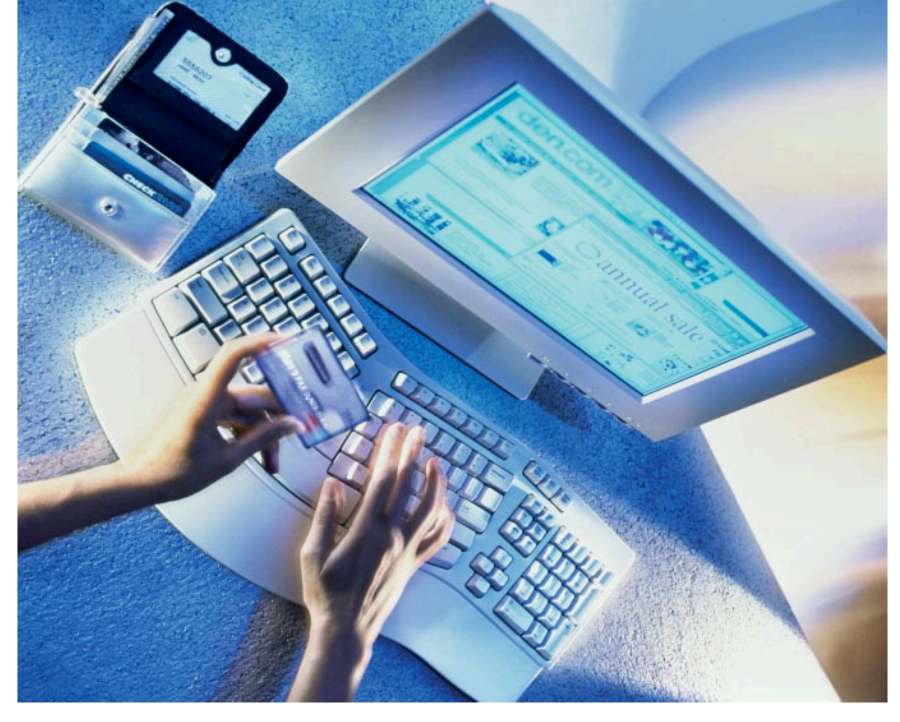
Quelques références :

- D. Krob et E.A. Vassilieva, « Performance evaluation of demodulation methods : a combinatorial approach », *Proceedings of DM-CCG, Discrete Mathematics and Theoretical Computer Science*, pp. 203-214 (2001) (disponible en ligne : http://dmtcs.loria.fr).
- X. Lagrange, P. Godlewski, S. Tabbane, *Réseaux GSM-DCS* (Hermès, 1997).
- J. G. Proakis, *Digital communications* (McGraw-Hill, 3e édition, 1995).
- C. Servin, *Télécoms : de la transmission à l'architecture de réseaux* (Masson, 1998).

Cryptage et décryptage : communiquer en toute sécurité

Jean-Louis Nicolas

Dans le monde actuel, où les télécommunications occupent une place cruciale, la cryptographie est un enjeu majeur. Elle est aussi devenue une science complexe, qui ne peut se passer de mathématiciens de haut niveau.



Payer avec sa carte de crédit, faire des achats sur Internet : les méthodes cryptographiques, qui mettent en jeu de belles mathématiques, sont indispensables à la sécurité de ces opérations. (Photo : Getty Images.)

En mars 2000, un gros titre avait fait la une des journaux : « Alerte à la sécurité des cartes bancaires ». Que s'était-il passé ? En France, le secret des cartes à puce était protégé depuis 1985 grâce à une méthode de cryptage faisant intervenir un grand nombre *N*, constitué de 97 chiffres. Ce nombre *N* doit être le produit de deux grands nombres premiers, c'est-à-dire de nombres qui, comme 7 ou 19, ne sont divisibles que par 1 et par eux-mêmes. Le secret d'une carte bancaire est constitué précisément par ce couple de nombres premiers ; les calculer à partir de *N* était pratiquement impossible dans la décennie 1980. Mais avec l'augmentation de la puissance des ordinateurs et l'amélioration des méthodes mathématiques, la taille des nombres *N* dont on peut calculer les facteurs premiers en un temps raisonnable a dépassé la centaine de chiffres dans les dernières années du siècle (le record actuel, 158 chiffres,

date de janvier 2002). Un informaticien astucieux, Serge Humpich, avait ainsi pu trouver les deux nombres premiers ultra-secrets dont le produit vaut *N* et les avait utilisés pour fabriquer de fausses cartes. Alors, pour garantir la sécurité de nos petits rectangles de plastique, l'organisme de gestion des cartes bancaires a aussitôt construit de nouveaux nombres *N*, nettement plus grands.

La cryptographie moderne, au croisement des mathématiques et de l'informatique

Cette péripétie illustre l'importance considérable que revêt aujourd'hui la science du cryptage, c'est-à-dire du codage de messages en vue de les rendre illisibles par des personnes indiscrètes. Crypter et décrypter des messages secrets est une activité vieille de plusieurs siècles, voire millénaires. Et cette activité a largement débordé du cadre strictement diplomatique ou militaire pour investir des pans entiers de l'univers des communications civiles : procédures d'authentification, transactions bancaires, commerce électronique, protection de sites et fichiers informatiques, etc.

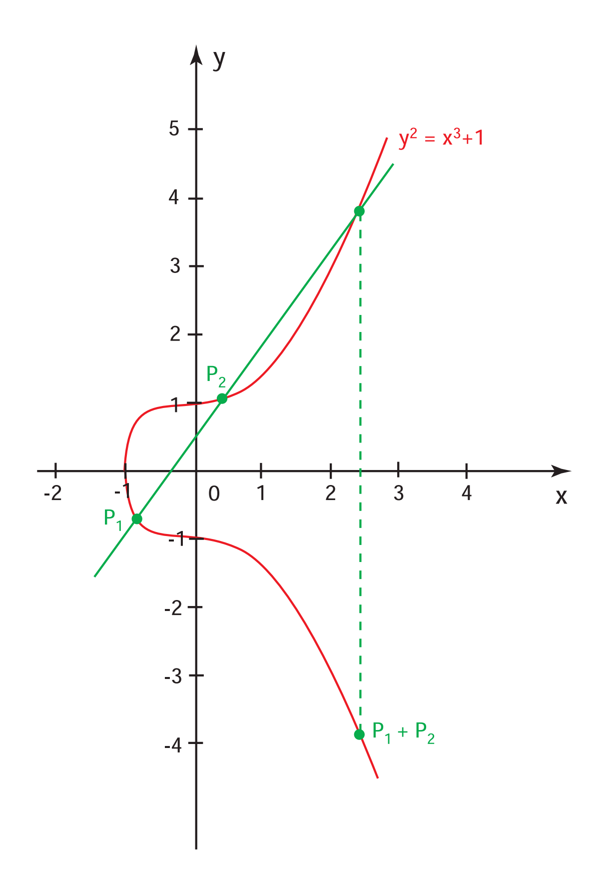
La cryptographie a connu beaucoup d'avancées au cours des dernières décennies. Ce faisant, elle est devenue une science complexe, où les progrès sont généralement le fait de spécialistes ayant reçu une formation poussée en mathématiques et en informatique. Cette spécialisation s'est manifestée dès la Deuxième guerre mondiale. On le sait aujourd'hui, le déchiffrage par les Alliés des messages codés par les fameuses machines allemandes *Enigma* a joué un rôle déterminant dans ce conflit. Or c'est un éminent mathématicien britannique, Alan Turing, par ailleurs l'un des pères de l'informatique théorique, qui a apporté une contribution essentielle à ce décryptage.

Dans les années 1970, la cryptographie a connu une petite révolution : l'invention de la cryptographie à « clé publique », avec la méthode RSA. De quoi s'agit-il ? Jusque-là, les correspondants voulant échanger des messages secrets devaient partager une clé secrète, et le risque d'interception de cette clé par l'ennemi était grand. Le protocole RSA, nommé ainsi d'après ses trois inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman), résout ce problème. Cette méthode utilise deux clés : une clé de cryptage publique — elle peut être connue de tous — et une clé de décryptage, qui reste secrète. Elle est fondée sur le principe (utilisé par la suite pour protéger les cartes bancaires, comme on l'a vu plus haut) qu'il est possible de construire de grands nombres premiers (de cent, mille chiffres, voire plus), mais qu'il est extrêmement difficile de retrouver les facteurs premiers p et q d'un grand nombre $N = p \times q$ lorsque l'on connaît seulement *N*. Schématiquement, la connaissance de *N* revient à celle de la clé publique de cryptage, tandis que la connaissance de p et q revient à celle de la clé secrète de décryptage.

Évidemment, si quelqu'un trouvait une méthode pour décomposer rapidement en leurs facteurs premiers de grands nombres, le protocole RSA deviendrait caduc. Mais il se pourrait aussi que les mathématiciens prouvent qu'une telle méthode n'existe pas, ce qui renforcerait la sécurité du protocole RSA. Ce sont là des sujets de recherche décisifs.

Les méthodes qui, comme le protocole RSA, font intervenir de la théorie des nombres élaborée, apportent une grande leçon : des

recherches mathématiques (sur les nombres premiers notamment) tout à fait désintéressées peuvent se révéler, des années ou des décennies plus tard, cruciales pour telle ou telle application ; et ce de manière imprévisible. Dans son livre *L'apologie d'un mathématicien*, le grand théoricien des nombres britannique G. H. Hardy (1877-1947), qui était un fervent pacifiste, se targuait de travailler dans un domaine parfaitement pur, l'arithmétique, et de n'avoir rien fait qui puisse être considéré comme « utile ». Ses travaux étaient peut-être « inutiles » à son époque. C'est faux aujourd'hui.

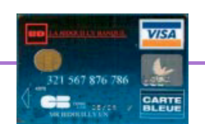


Le graphe de la courbe elliptique d'équation $y^2 = x^3 + 1$.
Les courbes elliptiques ont une propriété remarquable : on peut « additionner » leurs points selon le procédé représenté sur le dessin.
L'« addition » ainsi définie respecte les lois arithmétiques attendues, telles que $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Certaines méthodes modernes de cryptographie font appel aux courbes elliptiques et à leurs propriétés algébriques.

Courbes elliptiques : la géométrie algébrique au service des agents secrets

Et cela ne concerne pas uniquement la théorie des nombres. D'autres domaines des mathématiques, auparavant considérés comme dépourvus d'applications, contribuent à la science du cryptage. Des méthodes cryptographiques prometteuses et fondées sur des principes voisins de ceux du protocole RSA sont apparues au cours des dernières années. Il en est ainsi de la méthode dite du *logarithme discret*. Celle-ci a servi à son tour à concevoir des méthodes qui s'appuient sur les propriétés des *courbes elliptiques*. Il ne s'agit pas de courbes ayant la forme d'une ellipse, mais de courbes dont l'étude a débuté au XIXe siècle pour résoudre le problème difficile du calcul du périmètre d'une ellipse. Ces courbes, dont les coordonnées (x, y) de leurs points vérifient une équation de la forme $y^2 = x^3 + ax + b$, ont d'intéressantes propriétés — dont l'étude fait partie de la *géométrie algébrique*, très vaste domaine des mathématiques actuelles. Par exemple, à l'aide d'une construction géométrique appropriée, il est possible de définir une addition entre les points d'une courbe elliptique. Plus généralement, les objets géométriques que sont les courbes elliptiques possèdent des propriétés arithmétiques — que l'on continue d'explorer — susceptibles de rendre service à la cryptographie. C'est ainsi qu'a été développée une méthode cryptographique intitulée *logarithme discret sur les courbes elliptiques*.

Une autre direction s'est révélée récemment. Au congrès international des mathématiciens à Berlin en 1998, Peter Shor, des laboratoires AT & T, obtenait le prix Nevanlinna



pour ses travaux sur la *cryptographie quantique*. Que signifie ce terme ? Il y a quelques années, des physiciens et des mathématiciens ont imaginé qu'il serait un jour possible de réaliser un ordinateur quantique, c'est-à-dire dont le fonctionnement exploiterait les lois bizarres de la physique quantique, celles qui règnent dans le monde de l'infiniment petit. Or on s'est rendu compte qu'un tel ordinateur, s'il était réalisable, serait capable de factoriser très vite de grands nombres et rendrait ainsi inefficace la méthode RSA. Des recherches visant la réalisation concrète d'un ordinateur quantique ont d'ailleurs été publiées très récemment, dans la revue britannique *Nature* (*cf*. dernière référence ci-dessous). D'un autre côté, des chercheurs ont élaboré des protocoles de cryptographie quantique, c'est-à-dire des méthodes de cryptage utilisant des objets (photons, atomes,...) obéissant aux lois quantiques. Ces protocoles quantiques pourraient garantir une sécurité infaillible. Tout cela est à l'étude et risque de devenir opérationnel dans quelques années…

Jean-Louis Nicolas
Institut Girard Desargues, Mathématiques,
Université Claude-Bernard (Lyon 1)

Quelques références :

- D. Kahn, *La guerre des codes secrets* (Interéditions, 1980).
- J. Stern, *La science du secret* (Odile Jacob, 1998).
- S. Singh, Histoire des codes secrets (J.-C. Lattès, 1999).
- J.-P. Delahaye, *Merveilleux nombres premiers* (Belin/Pour la Science, 2000).
- D. Stinson, *Cryptographie, théorie et pratique* (Vuibert, 2001).
- L. M. K. Vandersypen et al., « Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance », *Nature, vol. 414*, pp. 883-887 (20 décembre 2001).

Contrôler un monde complexe



Pierre Perrier

Qu'il s'agisse de la manœuvrabilité d'un avion, de la tenue mécanique d'une structure compliquée ou de la gestion du trafic automobile, le progrès dans ces domaines ne vient pas uniquement des inventions purement techniques. Il naît aussi de recherches abstraites, comme la théorie mathématique du contrôle.

On comprend aisément l'intérêt de savoir contrôler la réaction d'un avion ou d'une fusée aux turbulences de l'écoulement de l'air, de déterminer la démarche à suivre en cas d'incident dans une centrale nucléaire, de gérer le réseau de distribution de l'électricité en cas de pannes, etc. Dans des situations normales, le contrôle vise à optimiser quelque chose, à améliorer des performances, à faire des économies de matériaux ou d'argent : c'est le cas lorsqu'on veut maintenir un satellite sur sa bonne orbite en utilisant le minimum de carburant.



Le pont Vasco de Gama sur le Tage, à Lisbonne. La résistance d'une structure complexe telle qu'un pont peut être contrôlée de façon active en plaçant, en des endroits bien choisis, des dispositifs qui vont, selon les mouvements de la structure, modifier ses caractéristiques mécaniques afin de contrecarrer les effets de résonance. La théorie mathématique du contrôle traite de telles situations. (Cliché Gamma/Gilles Bassignac)

Penchons-nous sur l'exemple de la gestion des pannes dans un réseau de distribution d'électricité. Un incident tel qu'un court-circuit ou une rupture de contact (due par

exemple à la chute d'un pylône), un surcroît de consommation d'énergie en un lieu donné, peut avoir sur le réseau une cascade de conséquences. Or il n'est généralement pas possible de réaliser une étude exhaustive de tous les incidents possibles, ni de calculer exactement chaque étape de la propagation de l'effet d'un tel incident. Le nombre de possibilités à explorer est gigantesque, en tout cas beaucoup trop élevé, même pour les ordinateurs les plus puissants. On est alors conduit à concevoir un modèle mathématique qui décrit de façon simplifiée le réseau et son fonctionnement. Moyennant des essais et des calculs d'ampleur raisonnable, une telle modélisation permet de cerner le comportement du système, au moins approximativement. En retour, cela peut aider à améliorer la conception des réseaux. Mais on voudrait aussi pouvoir *contrôler* une situation critique, provoquée par exemple par une surcharge localisée ou répartie sur une région entière. Autrement dit, on voudrait savoir quel est l'enchaînement des actions que le poste de commande doit effectuer afin de minimiser les conséquences de la panne. Une telle connaissance est-elle possible, en théorie ? Existe-t-il des stratégies de contrôle optimales ? Si oui, quelles sont-elles ? Et ensuite, quels algorithmes faut-il employer pour les vérifier par une simulation numérique, sur ordinateur, avant de tenter l'essai en grandeur réelle ?

Il est important de fournir un cadre d'étude rigoureux à ce problème de gestion des ressources, si l'on ne veut pas gaspiller l'énergie, ni être victime de coupures de courant généralisées. On a avec cet exemple un premier type de problèmes de contrôle complexe où les mathématiciens — à renfort de logique mathématique, de théorie des nombres, de théorie des probabilités, d'analyse et de théorie du contrôle — apportent leur contribution. À tout le moins, ils peuvent fournir quelques certitudes *a priori* quant à l'existence d'une solution acceptable et aux moyens de l'obtenir — solution que des expériences devront par la suite valider.

Empêcher les ponts de s'écrouler

La complexité n'est pas nécessairement rattachée à un réseau. Elle peut résider dans la manière dont réagit un objet, comme un pont. La tenue d'une telle structure dépend d'un grand nombre de paramètres, de son comportement vibratoire entre autres. Comme chacun sait, les vibrations d'un pont peuvent être provoquées par le passage de camions en file ou par le vent d'une tempête. Parfois, ce phénomène s'amplifie jusqu'à provoquer la rupture de l'ouvrage. Un pont, comme toute autre structure mécanique, possède une série de fréquences de vibration caractéristiques ; si la perturbation extérieure apporte de l'énergie à des fréquences qui correspondent aux fréquences propres de vibration, une *résonance* se produit et le pont accumule de l'énergie dans ses modes propres de vibration. Ceux-ci s'amplifient alors, tant que dure la perturbation extérieure, et tant que la structure résiste aux contraintes mécaniques qui en résultent.

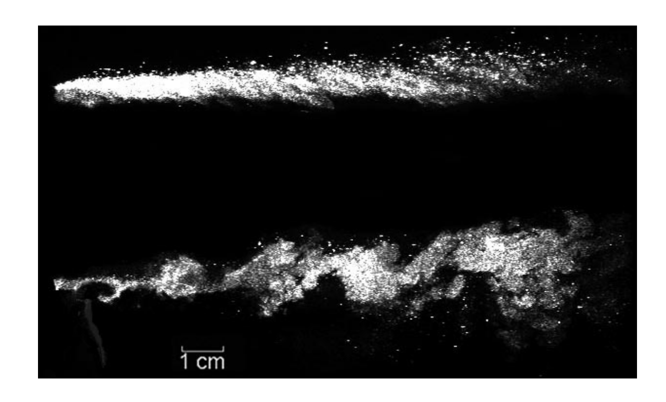
Pour contrôler de tels phénomènes, il faut les comprendre, savoir les prévoir et mettre en place des dispositifs techniques capables de contrecarrer les dangereuses résonances. On parle de *contrôle passif* lorsqu'on calcule où installer les amortisseurs qui absorberont assez d'énergie avant qu'elle ne s'accumule aux endroits critiques. Mais on parle de *contrôle actif* si, une fois repérés ces points critiques, on place en des endroits bien choisis des dispositifs actifs, des *actionneurs* ; ces derniers agiront

alors en fonction de l'amplitude des déplacements des points critiques, de façon à éviter toute évolution dangereuse de la structure. C'est une analyse mathématique du système étudié qui détermine les emplacements adéquats des capteurs et actionneurs et les procédures de contrôle les mieux adaptées.

Malheureusement, le calcul exact du comportement du système en l'absence de contrôle, de sa sensibilité et de son aptitude à être contrôlé est, le plus souvent, inaccessible. La raison est en général soit la complexité mathématique des problèmes dès qu'ils sont non linéaires (impossibilité de les décomposer en somme d'éléments simples et à peu près indépendants du point de vue mathématique), soit le temps de calcul sur ordinateur qui serait trop long. En conséquence, le contrôle est souvent imparfait. Il se peut par exemple que l'on réussisse à contrôler des modes de vibration provisoirement seulement — l'énergie extérieure s'accumule d'abord dans de nombreux modes de vibration de faible amplitude, avant de se combiner et de resurgir dans un nombre plus petit de modes, mais avec une forte amplitude. Beaucoup reste à faire pour bien comprendre ces processus et remédier à leurs effets négatifs.

Tenir bon malgré les turbulences

Prenons un troisième exemple : les écoulements de fluide à grande vitesse, comme l'écoulement de l'air autour d'un avion, d'une fusée en décollage, ou de l'eau autour d'un bateau rapide. Dans ces situations, on est confronté à la turbulence, c'est-à-dire à des mouvements complexes et instables du fluide, à une perpétuelle destruction et reconstruction de structures si compliquées qu'elles semblent relever d'un désordre total. Les turbulences peuvent gêner considérablement le mouvement d'un véhicule, aérien ou autre. On comprend que le contrôle soit ici beaucoup plus difficile à obtenir. Mais ces problèmes ont une grande importance pratique. Aussi les ingénieurs ont-ils essayé, par tâtonnements, et en s'inspirant par exemple du vol des oiseaux pour concevoir les avions, d'assurer une certaine contrôlabilité de l'écoulement. Ils y ont partiellement réussi en renforçant notamment les bords de fuite et d'attaque des ailes, en plaçant des capteurs en des endroits peu perturbés et des actionneurs — des gouvernes — aux endroits sensibles, près des bords de fuite.



L'image du haut montre un écoulement fluide supersonique relativement régulier. Dans l'image du bas, l'action d'un petit jet de fluide injecté latéralement a eu pour résultat le développement d'instabilités dans l'écoulement. Une telle manipulation illustre l'idée que l'on peut agir sur un écoulement à l'aide de petits dispositifs, notamment en vue de le contrôler (Cliché Erwan Collin-LEA/CEAT-Université de Poitiers).

La théorie mathématique du contrôle a permis dans un premier temps de retrouver ces résultats empiriques. Puis elle a permis de proposer des stratégies d'actions, des plans de conception qui renforcent ou diminuent, selon le cas, la sensibilité aux actions d'un opérateur humain ou aux perturbations extérieures. On en est maintenant au point d'identifier des dispositifs élémentaires de contrôle actif qui agiraient à l'échelle quasi microscopique, celle d'une couche de fluide de

quelques dixièmes de millimètre d'épaisseur : par exemple de petits volets ou des micro-mécanismes permettant de déformer localement le profil du véhicule aux points critiques de l'écoulement du fluide. En coordonnant l'action de très nombreux micro-dispositifs de ce genre, on obtiendrait, à l'échelle macroscopique, un écoulement fluide ayant les propriétés souhaitées. Dans le domaine du contrôle de la turbulence des fluides, des recherches mathématiques, alliées à des essais physiques ou techniques, vont ainsi ouvrir un monde de performances inimaginables il y a quelques années ; un monde où, pour obtenir un même effet, l'énergie ou la taille des dispositifs nécessaires sera diminuée de plus d'un ordre de grandeur.

La théorie du contrôle met en jeu divers champs mathématiques, en particulier la théorie des équations différentielles

Les problèmes de contrôle que l'on a évoqués ici peuvent concerner de banals essuie-glaces de voiture comme le lanceur spatial le plus élaboré. La théorie du contrôle, née dans les années 1940-1950 en relation notamment avec les activités aérospatiales, puise ses méthodes et ses concepts dans plusieurs branches des mathématiques. Elle concerne surtout des équations différentielles (où l'inconnue est une fonction) et des équations aux dérivées partielles (équations différentielles où la fonction inconnue est une fonction de plusieurs variables), un vaste champ d'étude déjà ancien mais toujours très actif. En effet, pour la plupart des systèmes rencontrés dans le monde réel, leur comportement peut être modélisé à l'aide d'une telle équation. Un problème de contrôle se traduit alors par une ou plusieurs équations différentielles ou aux dérivées partielles, qui contiennent des termes représentant des actions de contrôle, définies par l'homme. Notons globalement C ces termes de contrôle, et f la fonction représentant le comportement du système ; f est la solution d'équations différentielles où intervient C, et donc f dépend de C. Le but de la théorie du contrôle est alors, en gros, de déterminer le C adéquat pour que f, le comportement du système, soit acceptable. Pour un mathématicien, il ne s'agit pas tant de le faire avec telle ou telle équation particulière, mais plutôt d'obtenir des résultats généraux, valables pour de nombreuses classes d'équations et donc applicables à de nombreuses situations différentes.

En France, la théorie du contrôle figure en bonne place au sein de la brillante école de mathématiques appliquées qu'a su créer Jacques-Louis Lions (1928-2001). Mais à elle seule, une bonne école mathématique ne suffit pas. Il faut également que ses résultats soient connus et appliqués par tous ceux qui pourraient en avoir besoin. D'où l'intérêt de resserrer les liens entre la communauté mathématique et les mécaniciens, les ingénieurs, les chimistes ou les biologistes.

Pierre Perrier
Académie des sciences et
Académie des technologies, Paris.

Quelques références :

- J. R. Leigh, Control theory. A guided tour (Peter Peregrimus, Londres, 1992).
- J. Zabczyk, Mathematical control theory : an introduction (Birkhaüser, 1992).
- J.-L. Lions, Contrôlabilité exacte, perturbations et stabilisation de systèmes distribués (Masson, 1988).

Le théorème du soufflet

Étienne Ghys

Une règle, un crayon, du carton, des ciseaux et de la colle : il n'en faut guère plus pour procurer aux mathématiciens du plaisir et de jolis problèmes — dont l'étude se révèle souvent, après coup et de manière inattendue, utile dans d'autres métiers.

Construisons une pyramide en carton... Pour cela, on commence par découper un patron SABCDE dans une feuille de carton comme indiqué sur la figure 1, puis on plie le long des lignes pointillées et, enfin, on colle les côtés AS et ES.

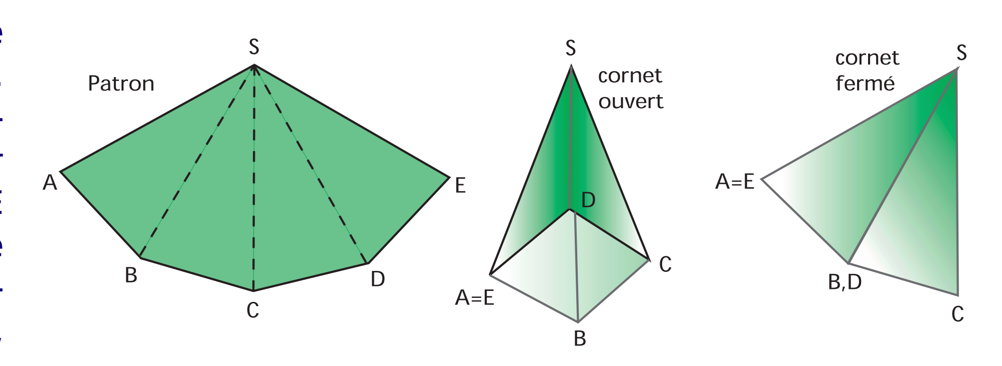


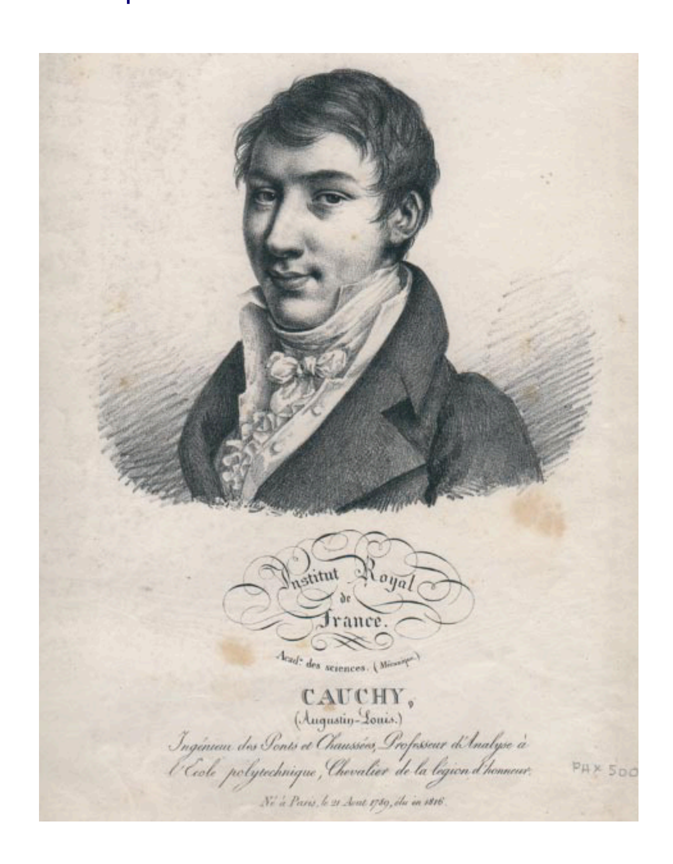
Figure 1. La construction d'une pyramide en carton. Dépourvu de la base ABCDA, cet objet est flexible.

Le résultat est une espèce de cornet dont le sommet est le point S et dont le bord est un quadrilatère ABCD. Cet objet est *flexible*. Si on le tient dans la main, le quadrilatère ABCD peut se déformer et s'ouvrir plus ou moins : la construction n'est pas très solide. Pour compléter la pyramide, il faut encore découper un carré en carton et le coller sur le quadrilatère pour former la base. Après cette opération, la pyramide est solidifiée, rigidifiée. Si on la pose sur une table, elle ne s'écroule pas. Si on la prend dans la main et si on essaye de la déformer (avec douceur !), on n'y parvient pas, à moins de déformer les faces en carton. De même, un cube en carton est *rigide* comme tout le monde l'a souvent constaté. Qu'en est-il pour un *polyèdre* plus général, possédant peut-être des milliers de faces ? La géode de la Villette, à Paris, est-elle rigide ? Cette dernière question laisse entrevoir que le sujet de la rigidité et de la flexibilité n'est peut-être pas seulement théorique !

Un problème encore d'actualité et qui remonte à l'Antiquité

Le problème de la rigidité de ce type d'objets est très ancien. Euclide en avait probablement connaissance. Le grand mathématicien français Adrien-Marie Legendre s'y est intéressé vers la fin du XVIIIe siècle et en a parlé à son collègue Joseph-Louis Lagrange ; lequel suggéra à son tour au jeune Augustin-Louis Cauchy d'étudier cette question en 1813. Ce sera le premier résultat marquant du baron A.-L. Cauchy, qui deviendra par la suite l'un des plus grands mathématiciens de son siècle.

Cauchy s'est intéressé aux polyèdres *convexes*, c'est-à-dire aux polyèdres qui n'ont pas d'arêtes rentrantes. Par exemple, la pyramide que nous avons construite ou le ballon de football sont convexes, tandis que l'objet dessiné à droite de la figure 2 ne l'est pas.



Augustin-Louis Cauchy (1789-1857), l'un des grands mathématiciens de son époque. (Cliché Archives de l'École polytechnique)

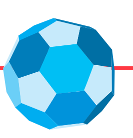



Figure 2. Un polyèdre convexe et un polyèdre étoilé, non convexe.

Le théorème établi par Cauchy est le suivant : *tout polyèdre convexe est rigide*. Cela signifie que si l'on construit un polyèdre convexe avec des polygones indéformables (en métal par exemple) ajustés par des charnières le long de leurs arêtes, la géométrie globale de l'ensemble empêche les jointures de jouer. Le cornet que nous avons construit est flexible mais cela n'invalide pas le théorème : il lui manque une face, et c'est la dernière face qui rigidifie la pyramide…

Faire des mathématiques, c'est *démontrer* ce qu'on affirme ! Or la démonstration de Cauchy est superbe (même si certains ont fait remarquer par la suite qu'elle était incomplète). Il n'est malheureusement pas question dans ce petit article de donner une idée de cette preuve, mais j'aimerais en extraire un « lemme », c'est-à-dire une étape dans la démonstration.

Posons sur le sol une chaîne constituée de quelques barres métalliques assemblées bout à bout, comme sur la figure 3. En chacun des angles de cette ligne polygonale, bougeons les deux barres de façon à diminuer l'angle correspondant. Alors, les deux extrémités de la chaîne se rapprochent. Cela vous semble évident ? Essayez de le démontrer…



Pendant longtemps, beaucoup de mathématiciens se sont demandé si les *polyèdres non convexes* étaient également rigides. Peut-on trouver une preuve de la rigidité qui n'utiliserait pas l'hypothèse de convexité ? Les mathématiciens aiment les énoncés dans lesquels toutes les hypothèses sont utiles pour obtenir la conclusion. Il a fallu attendre plus de 160 ans pour connaître la réponse dans ce cas particulier.



La géode de la Villette, à la Cité des sciences à Paris, est un polyèdre convexe formé de 1730 facettes triangulaires. La rigidité des polyèdres articulés donne lieu à un joli problème mathématique qui a été résolu seulement en 1997. (Cliché Cosmos/R. Bergerot)

En 1977, le mathématicien canadien Robert Connelly créa la surprise. Il a construit un polyèdre (assez compliqué) qui est flexible, bien sûr non convexe pour ne pas contrarier Cauchy ! Depuis, sa construction a été quelque peu simplifiée, en particulier par Klaus Steffen. Je présente dans la figure 4 un patron qui permettra au lecteur de construire le « flexidron » de Steffen. Découpez, pliez le long des lignes. Les lignes en continu sont des arêtes saillantes et les lignes en pointillé correspondent aux arêtes rentrantes. Collez les bords libres de la manière évidente. Vous obtiendrez une espèce de Shadok et vous verrez qu'il est effectivement flexible (un peu…).

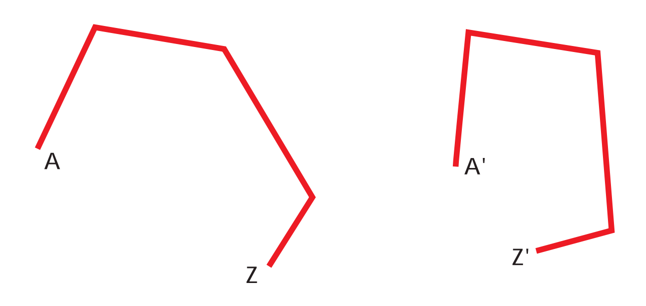


Figure 3. Si l'on diminue les angles que font les segments entre eux, les extrémités de la chaîne de segments se rapprochent.

Le volume d'un polyèdre varie-t-il lorsqu'on le déforme ?

À l'époque, les mathématiciens furent enchantés par ce nouvel objet. Un modèle métallique fut construit et déposé dans la salle de thé de l'Institut des hautes études scientifiques, à Bures-sur-Yvette près de Paris, et l'on pouvait s'amuser à faire bouger cette chose à vrai dire pas très jolie, et qui grince un peu. L'histoire raconte que Dennis Sullivan eut l'idée de souffler de la fumée de cigarette à l'intérieur du flexidron de Connelly et qu'il constata qu'en faisant bouger l'objet, aucune fumée ne sortait… Il eut donc l'intuition que quand le flexidron se déforme, son volume ne varie pas ! L'anecdote est-elle vraie ? Quoi qu'il en soit, Connelly et Sullivan conjecturèrent que *lorsqu'un polyèdre se déforme, son volume est constant*. Il n'est pas difficile de vérifier cette propriété dans l'exemple particulier du flexidron de Connelly ou encore pour celui de Steffen (au prix de calculs compliqués mais dépourvus d'intérêt). Mais la conjecture en question considère *tous* les polyèdres, y com-

pris ceux qui n'ont jamais été construits en pratique ! Ils ont appelé cette question la « conjecture du soufflet » : le soufflet au coin du feu éjecte de l'air quand on le presse ; autrement dit, son volume diminue (et c'est d'ailleurs sa fonction). Bien sûr, un vrai soufflet ne répond pas au problème de Connelly et Sullivan : il est en cuir et ses faces se déforment constamment, contrairement à nos polyèdres aux faces rigides.

En 1997, Connelly et deux autres mathématiciens, I. Sabitov et A. Walz, ont finalement réussi à prouver cette conjecture. Leur démonstration est grandiose, et illustre une fois de plus les interactions entre toutes les parties des mathématiques. Dans cette question éminemment géométrique, les auteurs ont utilisé des méthodes très fines d'algèbre abstraite moderne. Il ne s'agit pas d'une démonstration que Cauchy « aurait pu trouver » : les techniques mathématiques de l'époque étaient insuffisantes. Je voudrais rappeler une formule que l'on apprenait autrefois à l'école secondaire. Si les longueurs des côtés d'un triangle sont a, b et c, on peut calculer facilement la superficie du triangle. Pour cela, on calcule d'abord le demi-périmètre $p = (a + b + c)/2$ et ensuite on obtient la superficie en extrayant la racine carrée de $p(p - a)(p - b)(p - c)$. Cette jolie formule porte le nom du mathématicien grec Héron et nous vient de la nuit des temps. Peut-on calculer, de façon analogue, le volume d'un polyèdre si l'on connaît les longueurs de ses arêtes ? Nos trois mathématiciens contemporains ont montré que oui.

Ils partent d'un polyèdre construit à partir d'un patron formé d'un certain nombre de triangles et ils appellent l_1, l_2, l_3, etc. les longueurs des côtés de ces triangles (éventuellement très nombreux). Ils trouvent alors que le volume V du polyèdre doit satisfaire à une équation du n^e degré, c'est-à-dire une équation de la forme $a_0 + a_1V + a_2V^2 + \ldots + a_nV^n = 0$. Le degré n dépend du patron utilisé et les coefficients de l'équation (a_0, a_1, etc.) dépendent explicitement des longueurs des côtés l_1, l_2, l_3, etc. Autrement dit, si l'on connaît le patron et les longueurs des côtés, on connaît l'équation. Si le lecteur se souvient qu'une équation a en général une solution lorsqu'elle est du premier degré, deux solutions lorsqu'elle est du second degré, il pourra deviner qu'une équation de degré n n'a guère que n solutions. Conclusion : si l'on connaît le patron et les longueurs, on ne connaît pas nécessairement le volume, mais on sait au moins que ce volume ne peut prendre qu'un nombre fini de valeurs. Lorsque le flexidron se déforme, son volume ne peut donc pas varier continûment (sinon, le volume prendrait une infinité de valeurs successives) ; ce volume est « bloqué » et la conjecture du soufflet est établie...

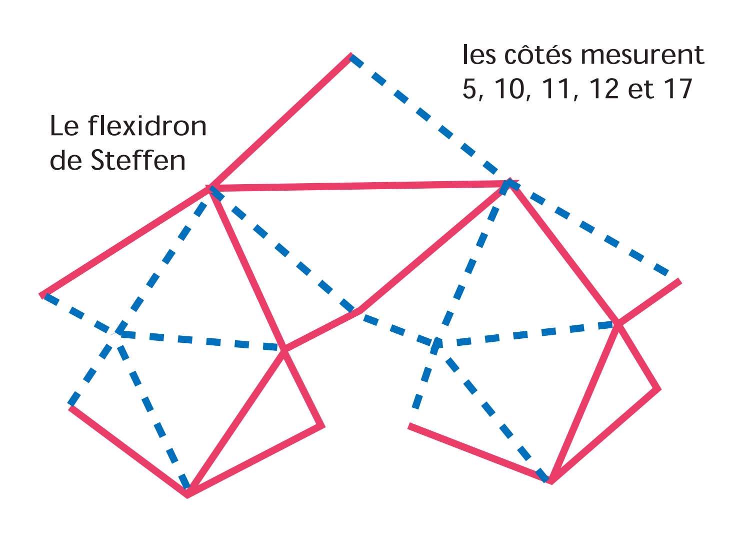
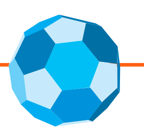


Figure 4. La patron du flexidron de Steffen.



Oui, le problème du soufflet est digne d'intérêt!

Ce problème est-il utile, intéressant ? Qu'est-ce qu'un problème mathématique intéressant ? Question difficile à laquelle les mathématiciens réfléchissent depuis longtemps, bien sûr. Voici quelques éléments de réponse, quelques indices de « qualité ». L'ancienneté est un premier critère : les mathématiciens sont très sensibles à la tradition, à des problèmes énoncés depuis longtemps, sur lesquels des mathématiciens de plusieurs générations ont planché. Un bon problème doit également s'énoncer simplement, sa solution doit mener à des développements surprenants, si possible mettant en relation des domaines très différents. De ces points de vue, le problème de la rigidité que nous venons d'aborder est intéressant.

La question de savoir si un bon problème doit avoir des applications utiles dans la pratique est plus subtile. Les mathématiciens y répondent de manière très variable. Incontestablement, les questions « pratiques », issues par exemple de la physique, servent bien souvent de motivation pour les mathématiques. Parfois, il s'agit de résoudre un problème bien concret, mais le lien est souvent plus flou : le mathématicien ne se sert alors de la question concrète que comme d'une *source d'inspiration* et la résolution effective du problème initial n'est plus la motivation véritable. Le problème de rigidité appartient à cette dernière catégorie. L'origine physique est assez claire : la stabilité et la rigidité de structures, par exemple métalliques. Pour l'instant, les exemples de Connelly ne sont d'aucune utilité pour les ingénieurs. Cependant, il paraît clair que ce genre de recherche ne manquera pas, dans un avenir indéterminé, de permettre une meilleure compréhension globale de la rigidité des vastes structures constituées d'un grand nombre d'éléments individuels (macromolécules, bâtiments, etc.). Il s'agit donc de recherches théoriques et « désintéressées », mais qui ont de bonnes chances de s'avérer utiles un jour…

Étienne Ghys
École Normale Supérieure de Lyon,
CNRS-UMR 5669

Quelques références :

- M. Berger, *Géométrie, vol. 3.* - Convexes et polytopes, polyèdres réguliers, aires et volumes (CEDIC/Nathan Information, 1977).
- R. Connelly, I. Sabitov, A. Walz, « The bellows conjecture », *Beiträge Algebra Geom., 38* (1997), n° 1, pp. 1-10.
- R. Connelly, « A counterexample to the rigidity conjecture for polyhedra », Institut des Hautes Études Scientifiques, *Publication Mathématique n° 47* (1977), pp. 333-338.
- N. H. Kuiper, « Sphères polyédriques flexibles dans E^3, d'après Robert Connelly », *Séminaire Bourbaki*, 30e année (1977/78), exposé n° 514, pp. 147-168 (Lecture Notes in Math. 710, Springer, 1979).

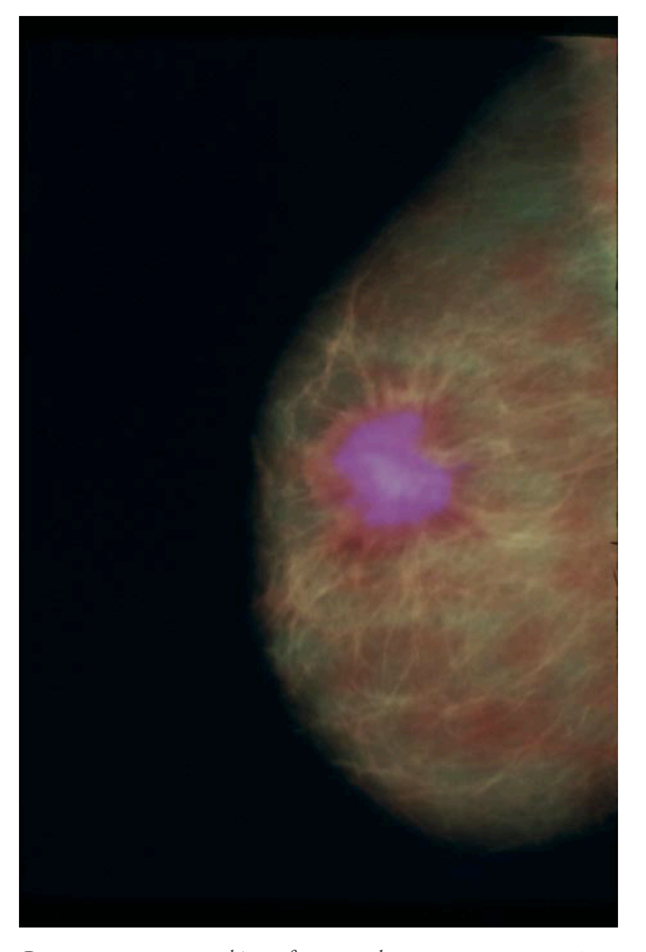
Trouver un gène responsable de cancer



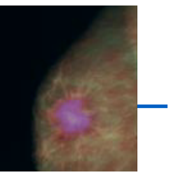
Bernard Prum

Les développements de la biologie moderne, et notamment ceux de la génétique moléculaire, exigent de nouveaux outils mathématiques. Exemple avec la statistique et son rôle dans la recherche d'un gène lié au cancer du sein.

D'innombrables maladies ont une composante héréditaire : le risque d'être atteint est plus ou moins élevé chez un individu selon qu'il est porteur ou non d'un gène dit de *susceptibilité* à la maladie en question. C'est pourquoi la génétique d'aujourd'hui cherche à comprendre le rôle des différents gènes, et en particulier leur rôle dans l'étiologie des maladies — dans l'espoir de mettre au point un jour une thérapie. Prenons comme exemple le cancer du sein qui, en France, touche ou touchera environ une femme sur huit. À côté de divers facteurs de risque (alimentation, tabac, exposition aux radiations, etc.), on a identifié il y a quelques années un gène dont les mutations sont impliquées dans un pourcentage élevé de femmes atteintes d'un tel cancer. Ce gène a été baptisé BRCA1 (pour *breast cancer 1*). Un tel résultat, de nature biomédicale, n'a pu être obtenu que par une succession d'analyses statistiques qui, nous allons le voir, ont permis de localiser le gène de façon de plus en plus précise.



Dans cette mammographie en fausses couleurs, une tumeur cancéreuse est visible en rose. Une partie des recherches sur les cancers du sein sont consacrées à leur aspect génétique. La théorie des statistiques y joue un rôle capital. (Cliché Kings College School/SPL/Cosmos)



La génétique a longtemps ignoré la nature matérielle des gènes. Ce n'est que depuis une vingtaine d'années que l'on a accès massivement aux séquences d'ADN, la chaîne moléculaire qui matérialise l'information génétique transmise des parents aux enfants. Pour autant, l'ignorance de la composition chimique des gènes n'a nullement empêché d'obtenir des résultats fins sur l'hérédité de tel ou tel trait.

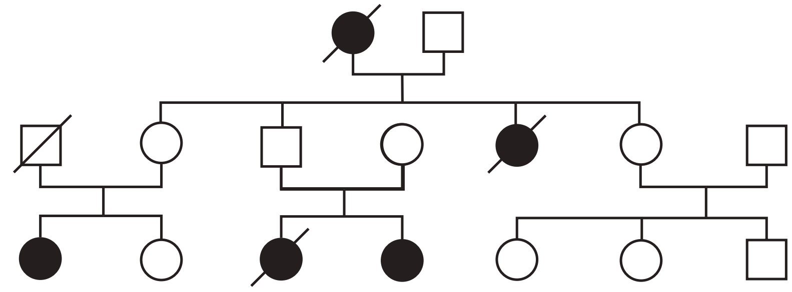


Figure 1. Une famille où l'on observe une concentration de cancers du sein. Les carrés indiquent les hommes, les cercles les femmes. Un individu est indiqué en noir s'il est atteint, barré s'il est décédé. On constate que la grand-mère, une de ses filles et trois de ses petites filles ont eu un cancer. Bien sûr, chez d'autres membres de la famille, la maladie peut encore se déclarer. C'est à partir de tels pedigrees que les généticiens sont conduits à supposer l'existence de gènes de susceptibilité à la maladie.

La première question que l'on se pose face à une maladie comme le cancer du sein est : « est-ce une maladie génétique, existe-t-il des gènes qui prédisposent à cette maladie ? ». Pour les cancers, la réponse a longtemps été incertaine. On s'attend à une réponse positive si l'on constate des concentrations familiales de la maladie, si l'on peut attribuer à la fille ou la sœur d'une femme atteinte un risque plus grand que celui encouru par l'ensemble de la population. Et pendant longtemps, le statisticien généticien a eu pour données de base des *pedigrees* comme celui de la figure 1.

Que faire d'un tel pedigree ? On sait, presque depuis Mendel, qu'un caractère héréditaire est souvent déterminé par un « gène » pouvant prendre plusieurs formes, appelées ses *allèles*. Chaque individu hérite un allèle de son père et un allèle de sa mère ; il transmet à chacun de ses enfants l'un de ces deux allèles au hasard. Le généticien propose alors, pour la transmission de la maladie étudiée, un modèle, qui suppose l'intervention de certains gènes et allèles. Ce modèle, le statisticien doit le valider à l'aide de tests statistiques appropriés, qui permettront par exemple d'éliminer les hypothèses les plus simples, comme : « la maladie étudiée n'a aucune composante génétique ».

Dans le cas de plus en plus étudié des maladies à étiologie complexe (cas du cancer du sein), où interviennent des facteurs d'environnement ou bien dont l'incidence dépend de l'âge, il convient de traiter des données qui dépendent du temps ; on doit alors faire appel à la *statistique des processus*. C'est une branche mathématique élaborée, qui s'appuie en grande partie sur les résultats obtenus par l'école française de probabilités des années 1980 (P. A. Meyer, J. Jacod) et ceux de statistique dus à l'école scandinave.

Des statistiques pour déterminer le chromosome porteur du gène

Une fois établie par l'analyse des pedigrees l'existence d'un gène de susceptibilité au cancer du sein, la seconde étape consiste à le localiser, au moins grossièrement, sur l'un des 23 chromosomes humains. Pour cela, on dispose depuis les années 1980 de *marqueurs* ; ce sont de petites chaînes d'ADN bien déterminées que l'on peut « lire » à moindre coût, disons par une analyse chimique rapide. Balises

relativement faciles à localiser, les marqueurs permettent par exemple d'évaluer la ressemblance entre des régions de chromosomes examinées chez des personnes malades et apparentées. Plus grande est la similitude d'une même région de chromosome chez des personnes apparentées atteintes, plus élevée est la probabilité que cette région porte un gène impliqué dans la maladie.

Mais une telle analyse, statistique bien sûr, est compliquée par le fait que chaque parent ne transmet pas à ses enfants les chromosomes qu'il a lui-même hérités de ses parents, mais une *recombinaison* de ceux-ci (figure 2). Si l'on considère deux gènes situés au départ sur un même chromosome, ils pourront après recombinaison se retrouver sur deux chromosomes différents ; la probabilité que cela arrive est d'autant plus élevée que les deux gènes en question sont éloignés. Analyser le taux de similarité le long d'un chromosome, c'est donc étudier un processus aléatoire. Grâce à la statistique des *processus*, on peut donc délimiter un intervalle dans lequel se trouve un gène de susceptibilité. L'emploi des marqueurs a ainsi permis à l'équipe américaine de Jeff M. Hall, à Berkeley, de localiser en 1990 le gène BRCA1 sur le chromosome 17.

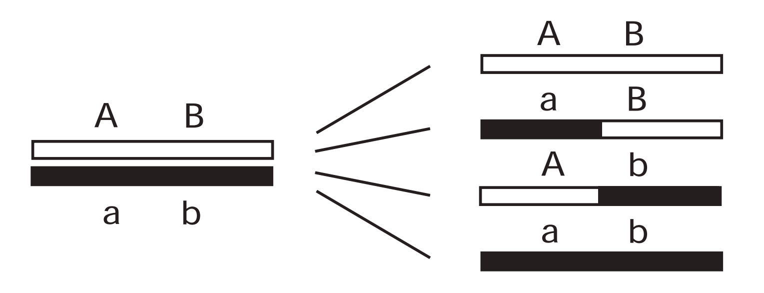


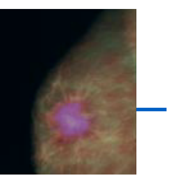
Figure 2. Pour chaque paire de chromosomes d'un individu, un chromosome est hérité de son père (en noir) et l'autre hérité de sa mère (en blanc). Un parent transmet à chaque descendant un seul chromosome de chaque paire. Mais avant la transmission, les chromosomes de chaque paire peuvent s'échanger des morceaux, au hasard. Ce processus dit de recombinaison fait que le parent transmet à son enfant un chromosome recombiné (l'une des quatre possibilités indiquées dans la figure, où l'on suppose que les chromosomes s'échangent deux régions).

Lire la molécule d'ADN pour décrire complètement le gène et ses formes anormales

Il s'agit ensuite de localiser précisément le gène et de déterminer sa structure. On sait que l'ADN, le matériau génétique, est une longue chaîne moléculaire « écrite » dans un alphabet de 4 « lettres » (*a*, *c*, *g* et *t*, initiales des quatre types de molécules dont est formée la chaîne d'ADN). Les banques de données génétiques répertorient plusieurs milliards de telles lettres (il en arrive quelque 25 millions par jour...).

La précision de la méthode des marqueurs permet au mieux de localiser un gène sur une séquence d'ADN comptant quelque 4 millions de lettres. Pour savoir exactement quel allèle, ou quelle mutation est responsable, par exemple, du cancer du sein, il faut « lire » ces séquences chez les sujets sains et malades pour les comparer. Cela revient à trouver une « faute de frappe » dans un texte de 4 millions de caractères, disons un livre de 2000 pages – ou plutôt dans autant de livres de 2000 pages que l'on a d'individus à étudier. Cette tâche est lourde, même avec des moyens informatiques puissants. Or chez l'homme, les gènes ne constituent pas plus de 3 % des chromosomes. Le reste du matériel chromosomique est qualifié d'*intergénique*. Si l'on parvient à limiter la recherche des fautes de frappe aux seuls gènes, on réduit la séquence à explorer à une trentaine de pages, ce qui devient accessible à tout ordinateur.

Mais comment distinguer les gènes



du reste ? Il s'avère que le « style » dans lequel sont écrits les gènes diffère du style intergénique : les fréquences de successions de lettres ne sont pas les mêmes. On peut chercher à exploiter cette différence de style pour *annoter* la séquence et distinguer les gènes de la partie intergénique. Le défi est ardu. On doit faire appel à des modèles statistiques appelés *chaînes de Markov cachées* et développés dans les années 1980, en liaison notamment avec des problèmes de reconnaissance automatique de la parole ; ils ont dû être adaptés à la génomique, en même temps que l'on mettait au point des algorithmes capables à la fois de caractériser les différents styles et d'attribuer un style à chaque position sur le chromosome.

C'est ainsi que l'on a fini par localiser précisément BRCA1. On peut désormais le lire facilement chez chaque malade. Ce gène de susceptibilité au cancer du sein compte 5 592 lettres et l'on en connaît plus de 80 allèles. Reste un nouveau travail pour le statisticien : établir les relations entre les divers allèles et la prévalence de ce cancer.

La biologie offre aux mathématiques un nouveau terrain d'action

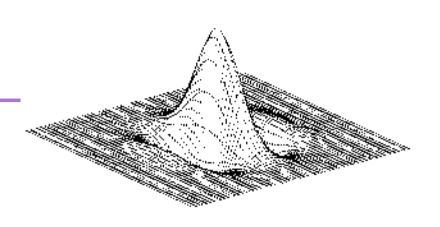
L'exemple du gène BRCA1 le suggère, la biologie jouera probablement vis-à-vis des mathématiques le rôle détenu par la physique au cours d'une bonne partie du XXe siècle : offrir un champ d'application aux outils théoriques récents et susciter l'élaboration de nouveaux outils (nous avons évoqué ici les outils statistiques, mais on pourrait évoquer d'autres domaines des mathématiques comme les systèmes dynamiques, l'optimisation, jusqu'à la géométrie — la conformation spatiale des molécules joue, on le sait, un rôle essentiel dans leur fonction). Un nouveau défi est aujourd'hui lancé au statisticien : on est actuellement capable de placer quelques milliers de réactifs sur une surface de verre d'un centimètre carré (les « puces ») et de savoir ainsi quels gènes travaillent dans quels tissus, dans quelles conditions expérimentales ou… dans quelles cellules cancéreuses. Les mesures effectuées en laboratoire, selon des centaines de conditions diverses, fournissent aux chercheurs un nombre considérable de données numériques, qui caractérisent l'expression de milliers de gènes. À ce jour, seules des analyses statistiques peuvent prétendre les traiter et préciser ainsi les liens entre gènes et maladies.

Bernard Prum
Laboratoire Statistique et Génome
(UMR CNRS 8071),
La Génopole, Université d'Évry

Quelques références :

- B. Prum, « Statistique et génétique » dans *Development of Mathematics 1950-2000* (sous la dir. de J.-P. Pier, Birkhäuser, 2000).
- C. Bonaïti-Pellié, F. Doyon et M. G. Lé, « Où en est l'épidémiologie du cancer en l'an 2001 », *Médecine-Science, 17,* pp. 586-595 (2001).
- F. Muri-Majoube et B. Prum, « Une approche statistique de l'analyse des génomes », *Gazette des mathématiciens, n° 89*, pp. 63-98 (juillet 2001).
- B. Prum, « La recherche automatique des gènes », *La Recherche, n° 346*, pp. 84-87 (2001).
- M. S. Waterman, *Introduction to computational biology* (Chapman & Hall, 1995).

Des ondelettes pour comprimer une image



Stéphane Mallat

Qu'elles soient stockées numériquement dans des mémoires informatiques ou qu'elles voyagent à travers Internet, les images occupent beaucoup de place. Heureusement, il est possible de les « condenser » sans altérer leur qualité !







Figure 1. Ces trois images illustrent la puissance des méthodes de compression actuelles. L'image originale (A) est constituée de 512 x 512 points, chacun d'eux ayant un certain niveau de gris, pris dans une palette de 256 niveaux. L'image (B) est le résultat d'une compression par un facteur 8, réalisée en réduisant les niveaux de gris à 2 valeurs possibles seulement (noir ou blanc). L'image (C) a été obtenue de (A) par une compression d'un facteur 32 en utilisant une base d'ondelettes. La différence de qualité avec l'image initiale est à peine perceptible. (Illustration auteur)

Une image numérisée se comprime, tout comme un jus d'orange que l'on réduit à quelques grammes de poudre concentrée. Il ne s'agit pas d'un tour de passe-passe, mais de techniques mathématiques et informatiques permettant de réduire la place occupée par une image dans un ordinateur ou dans un câble de communication. Elles sont aujourd'hui indispensables pour stocker de l'information ou la transmettre par Internet, téléphone, satellite ou autre.

La compression d'une image revient à représenter celle-ci à l'aide d'un nombre réduit de paramètres, en éliminant les redondances. Un exemple caricatural aidera à comprendre l'idée de principe : dans le cas d'une image uniformément blanche, il est inutile de préciser explicitement pour chacun de ses points le niveau de gris correspondant ; cela serait beaucoup plus long que d'énoncer : « tous les points de l'image sont blancs ». Le problème de la représentation est un sujet central en mathé-

matiques, et ses applications vont bien au-delà de la compression de données. Durant ces dix dernières années, des avancées considérables ont eu lieu grâce au développement de la théorie des *ondelettes*. Dans le domaine du traitement d'images, ces progrès ont abouti à l'adoption du nouveau standard de compression JPEG-2000. Cette histoire a de nombreux méandres, qui illustrent bien le rôle des mathématiques dans le paysage scientifique et technologique moderne.

Trente-deux fois moins de place grâce aux ondelettes

Considérons une image comme celle de la figure 1A. Elle est constituée de 512 x 512 points, dont les niveaux de gris peuvent varier de 0 (noir) à 255 (blanc). Chacun des 256 niveaux de gris possibles peut être représenté par un octet, c'est-à-dire un nombre binaire constitué de 8 bits (un octet est donc simplement une suite de 8 chiffres 0 ou 1, comme 11 010 001). Il faut donc 512 x 512 x 8 = 2 097 152 bits pour coder une seule image de ce genre, ce qui est beaucoup ! Première idée qui vient à l'esprit pour réduire le nombre de bits : diminuer le nombre de niveaux de gris, par exemple en se limitant à du blanc ou du noir, comme dans la figure 1B. Les deux valeurs possibles du niveau de gris se codent avec un seul bit (valant 0 ou 1), et l'on a ainsi diminué le nombre de bits par 8. Évidemment, la qualité de l'image s'est beaucoup dégradée. Regardez maintenant l'image de la figure 1C. Elle est codée avec 32 fois moins de bits que l'image originale, par une méthode utilisant la théorie des ondelettes ; pourtant, la dégradation est à peine perceptible ! Pourquoi ? Parce qu'au lieu de réduire la précision, c'est la manière de représenter l'information qui a ici été changée.

Au commencement était l'analyse de Joseph Fourier…

Comme on l'a dit, l'image numérisée est définie par les 512 x 512 nombres qui spécifient l'intensité lumineuse en chaque point. On peut donc interpréter cette image comme un point dans un espace à 512 x 512 dimensions — de la même façon qu'un point sur une surface, espace à deux dimensions, peut être repéré par deux coordonnées — et se demander quels sont les axes de coordonnées les plus appropriés pour représenter un tel point. Un système d'axes (ici de nature plus abstraite que les axes familiers de la géométrie élémentaire) définit ce que l'on appelle une *base*.

Une première avancée fondamentale a été réalisée par le mathématicien-physicien Joseph Fourier en 1802, dans son mémoire à l'Académie des Sciences sur la propagation de la chaleur, sujet *a priori* sans relation avec notre problème. Fourier a notamment montré que, pour représenter de façon compacte et commode une fonction *f(x)* (du point de vue mathématique, une telle fonction est un point dans un espace ayant une infinité de dimensions), on peut utiliser des « axes » construits à l'aide d'un ensemble infini de fonctions sinusoïdales. En des termes un peu plus précis : Fourier a montré que l'on peut représenter une fonction *f(x)* par une somme d'une infinité de fonctions sinus et cosinus de la forme sin (*ax*) ou cos (*ax*), chacune affectée d'un certain coefficient.

Ces « bases de Fourier » sont devenues un outil essentiel, d'usage extrêmement fréquent dans les sciences, car elles servent à représenter de nombreux types de fonctions, donc de nombreuses grandeurs physiques. En particulier, on les utilise aussi pour représenter

des sons ou des images. Et pourtant, les ingénieurs savent bien que ces sinusoïdes sont loin d'être idéales pour des signaux aussi complexes que des images : elles ne représentent pas efficacement des structures transitoires telles que les contours de l'image.

…puis est venue la « transformée en ondelettes »

Les spécialistes du traitement des signaux n'étaient pas les seuls à prendre conscience des limitations des bases de Fourier. Dans les années 1970, un ingénieur-géophysicien français, Jean Morlet, s'est rendu compte qu'elles n'étaient pas le meilleur outil mathématique pour explorer le sous-sol ; cela conduisit à l'une des découvertes — dans un laboratoire d'Elf-Aquitaine — de la *transformée en ondelettes*. Cette méthode mathématique, fondée sur un ensemble de fonctions de base différentes des fonctions sinusoïdales utilisées dans la méthode de Fourier, remplace avantageusement la *transformée de Fourier* dans certaines situations. Par ailleurs, dès les années 1930, les physiciens s'étaient rendu compte que les bases de Fourier n'étaient pas bien adaptées pour analyser les états d'un atome. Cela a été à l'origine de nombreux travaux qui ont, ultérieurement, beaucoup apporté à la théorie des ondelettes. C'est aussi vers les années 1930 que des mathématiciens se sont mis à tenter d'améliorer les bases de Fourier pour analyser des structures singulières localisées, ce qui a ouvert un important programme de recherche toujours très vivant. Autrement dit, une multitude de communautés scientifiques ont développé, avec les moyens du bord, des modifications des bases de Fourier. Dans les années 1980, Yves Meyer, un mathématicien français, a découvert les premières bases d'ondelettes orthogonales (l'orthogonalité désigne une propriété qui facilite beaucoup les raisonnements et les calculs ; les bases de Fourier sont également orthogonales). Cette découverte, suivie de quelques rencontres inopinées autour de photocopieuses ou de tables de café, ont déclenché en France un vaste mouvement scientifique pluridisciplinaire, dont l'impact international fut considérable. Les applications de la théorie et des algorithmes d'ondelettes ont fait leur chemin non seulement dans de nombreux domaines scientifiques et technologiques, mais sont aussi à l'origine de la création de plusieurs entreprises aux États-Unis.

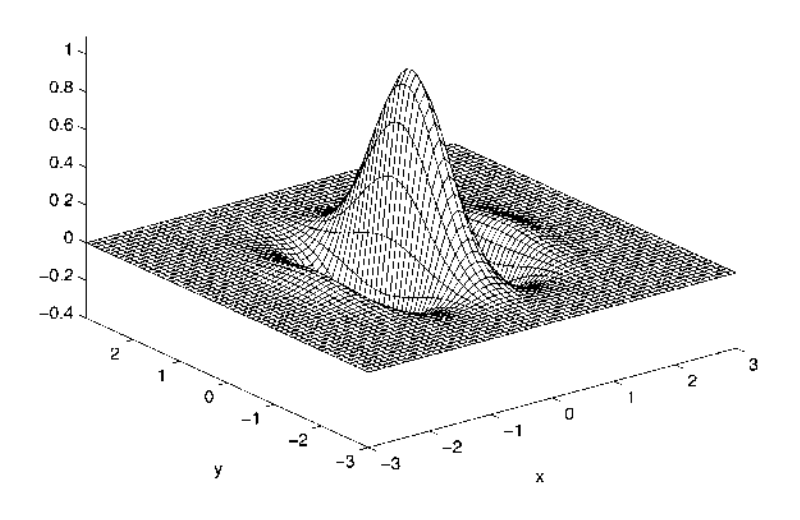


Figure 2. Le graphe d'une ondelette utilisée dans la compression d'images.

Les mathématiques des ondelettes ont joué un rôle de pivot dans nombre de domaines

Les mathématiques ont eu ici un rôle fondamental, à la fois de catalyse, de nettoyage et d'approfondissement. En dégageant les concepts fondamentaux des appli-

cations spécifiques, elles ont permis à des scientifiques de domaines très divers — en physique, en traitement du signal, en informatique, etc. — de se rendre compte qu'ils travaillaient sur le même outil. Aller au-delà, affiner ces outils, contrôler leurs performances : ce sont les travaux mathématiques modernes sur l'analyse de Fourier qui ont rendu tout cela possible. Enfin, cette théorie a donné une technique standard de calcul scientifique (la *transformée en ondelettes rapide*) grâce à une collaboration entre mathématiciens et spécialistes du traitement des signaux. L'image de la figure1C a ainsi été obtenue grâce aux mêmes bases d'ondelettes que celles utilisées en statistique, en sismique, ou en calcul scientifique, avec le même algorithme rapide. Et à travers le standard international JPEG-2000 pour la compression d'images, ces ondelettes envahissent actuellement tous les domaines de l'image, de l'Internet aux appareils photos numériques, et se dirigent vers les satellites.

Un pont reste à construire entre le monde des ondelettes et le monde de la géométrie

Les bases de Fourier n'étaient pas bien adaptées à l'analyse des phénomènes transitoires, tandis que les bases d'ondelettes le sont. Est-ce la fin de l'histoire ? Non. En traitement d'images, comme dans tous les autres domaines où les ondelettes sont devenues un outil de base, chacun bute actuellement sur le même type de problème : exploiter les régularités géométriques. En effet, on sait qu'une image, même complexe, est remarquablement bien représentée par un simple dessin composé de relativement peu de traits, et l'on peut souvent assimiler les contours des objets figurant dans l'image à des courbes géométriques assez simples. Mettre à profit ces courbes et leur régularité devrait donc permettre d'améliorer considérablement les résultats obtenus jusqu'à présent ; mais la théorie des ondelettes n'en est pour l'instant pas capable. Construire ce pont avec le monde de la géométrie pose des problèmes mathématiques difficiles. Cependant, l'enjeu scientifique et industriel étant important, on peut s'attendre à ce qu'il soit construit dans les dix années à venir. En France ?

Stéphane Mallat
Département de mathématiques appliquées,
École polytechnique, Palaiseau

Quelques références :

- B. B. Hubbard, *Ondes et ondelettes - La saga d'un outil mathématique* (Pour la Science/Belin, 1995).
- S. Mallat, *Une exploration des signaux en ondelettes* (École polytechnique/Ellipses, 2000).
- Y. Meyer, *Ondelettes et algorithmes concurrents* (Hermann, 1992).

Empêcher les ondes de faire du bruit

Daniel Bouche



Comment échapper à la détection par un radar? Quelle est la forme optimale d'un mur anti-bruit? Peut-on améliorer les images échographiques? Pour recevoir une réponse satisfaisante, ces questions demandent des analyses théoriques poussées.

Qu'est-ce qu'une onde ? Bien malin celui qui saurait donner une réponse à la fois précise et unique à cette question ! Pourtant, les ondes sont omniprésentes et constituent le quotidien d'un grand nombre de scientifiques et d'ingénieurs. En termes un peu vagues et intuitifs, on peut dire qu'une onde est la propagation d'un signal, d'une perturbation, dans un certain milieu, à une vitesse identifiable.

Les exemples ne manquent pas. Il y a bien sûr les vaguelettes que l'on peut créer à la surface de l'eau en y jetant un petit caillou; ici, c'est une perturbation de la hauteur de l'eau qui se propage. La distance entre deux vaguelettes successives est la *longueur d'onde*, une grandeur fondamentale dans la description des phénomènes ondulatoires. Les ondes sonores, elles, mettent en jeu des variations de la pression et de la densité du milieu ambiant (l'air le plus souvent), ces variations se produisant à des fréquences *audibles*. Les ondes acoustiques sont de même nature, et englobent à la fois les ondes sonores et celles que l'oreille ne perçoit pas. Lorsqu'elles se propagent au sein d'un solide, on parle plutôt d'ondes élastiques, dont font partie les ondes sismiques qui traversent l'intérieur de notre planète et que détectent les sismographes.

Le cas des ondes électromagnétiques est particulièrement important. Ce sont des variations de champs électrique et magnétique, qui se propagent dans le vide à la vitesse de la lumière. La lumière visible, les infrarouges, les ultraviolets, les rayons X, les rayons gamma, les micro-ondes, les ondes radio, les ondes radar, tous ces phénomènes sont des ondes électromagnétiques. Ce qui les distingue, c'est leur fréquence, ou encore leur longueur d'onde (quelques fractions de micromètre pour la lumière visible, encore moins pour les ultraviolets et les rayons X et gamma, quelques centimètres à quelques centaines de mètres pour les ondes radar et radio).

L'étude du comportement des ondes sert non seulement à comprendre la nature qui

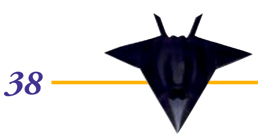
nous entoure, mais aussi à maîtriser quantité de techniques, et *a fortiori* à créer de nouvelles inventions pointues. Le comportement des ondes lumineuses touche tout le domaine des instruments optiques, qu'il s'agisse d'objectifs photographiques, de microscopes, d'appareils de télémétrie, etc. On peut penser aux ondes radar et à leurs applications militaires, à la conception d'engins militaires furtifs, c'est-à-dire qui échappent autant que faire se peut à la détection par les radars. Quant aux ondes acoustiques, on peut évoquer la conception de salles de concert ayant une acoustique optimale, de matériaux ou de structures absorbant le bruit, de dispositifs anti-bruit actifs (c'est-à-dire qui émettent des ondes sonores opposées à celles du bruit, pour neutraliser celui-ci), d'appareils d'échographie ou de destruction de calculs rénaux, d'appareils de contrôle non destructif (détection de défauts dans des pièces d'avions par exemple), etc.

Le Petit duc est un drone (petit avion télécommandé) que développe Dassault Aviation. C'est un appareil furtif : sa forme et ses matériaux sont choisis de manière à ce qu'il soit difficile à détecter par les ondes radar. Ce choix s'effectue sur la base de calculs compliqués portant sur la propagation d'ondes ; dans certains cas, la précision de tels calculs laisse à désirer et fait l'objet de recherches soutenues (Cliché Dassault Aviation).

Des équations connues, mais difficiles à résoudre avec précision

Les équations qui régissent les différents types d'ondes sont bien connues depuis longtemps. Ainsi, celles relatives aux ondes électromagnétiques ont été établies par le physicien écossais James Clerk Maxwell il y a plus d'un siècle, vers 1870. Mais il ne suffit pas de connaître les équations auxquelles obéit une onde radar, par exemple, pour savoir comment cette onde va se propager, interagir avec l'obstacle — constitué par un avion ou un autre objet que l'on cherche à détecter et à localiser — et se réfléchir partiellement vers l'antenne radar qui l'a émise. Il faut en effet pouvoir résoudre ces équations, dont l'inconnue est le champ ondulatoire, c'est-à-dire les amplitudes de l'onde en chaque point de l'espace et à tout instant. Ce n'est pas du tout facile. Il s'agit d'*équations aux dérivées partielles* (où interviennent l'amplitude inconnue de l'onde et ses dérivées par rapport aux coordonnées spatiales et au temps), que l'on doit compléter par des « conditions aux limites ». Celles-ci spécifient mathématiquement des données essentielles comme le champ ondulatoire à l'instant initial, la forme de l'obstacle et la façon dont l'onde se comporte à sa surface (réflexion, absorption, etc.), la manière dont l'amplitude de l'onde décroît à très grande distance de la source et de l'obstacle.

La résolution de ce type de problèmes, où l'onde est diffractée (déviée, modifiée) par des objets, est complexe ; elle nécessite des outils mathématiques, certains simples et connus depuis longtemps, d'autres beaucoup plus élaborés et encore en développement. Plus



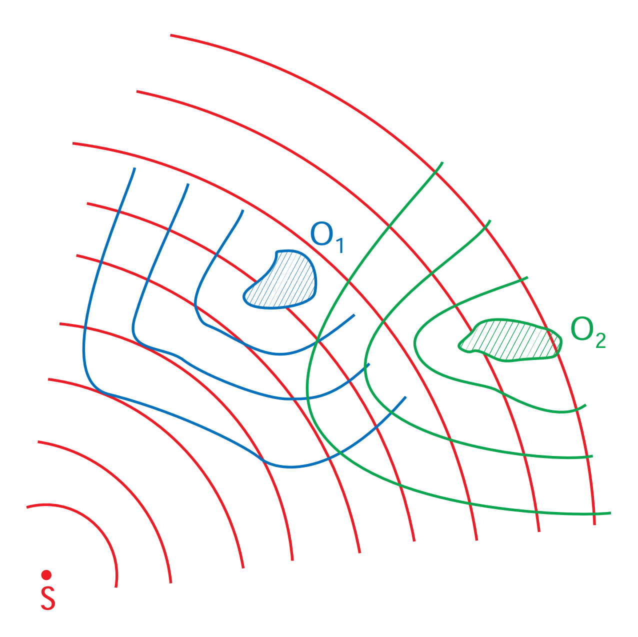
généralement, d'ailleurs, les équations aux dérivées partielles représentent une branche très importante des mathématiques, qui fait l'objet de recherches actives depuis plus de deux cents ans. Une fois les équations et leurs conditions aux limites établies, l'une des premières tâches du mathématicien consiste à formuler le problème en termes rigoureux et à démontrer que les équations ont une solution, et que si c'est le cas, la solution est unique (autrement, cela signifierait que le problème est mal posé, que la modélisation est incomplète). Une telle étude peut être ardue, et on ne sait pas toujours la mener à bien ; mais elle permet de s'assurer que l'on ne se lancera pas en vain dans des calculs de résolution !

L'analyse mathématique permet de formuler rigoureusement le problème et de mettre au point des méthodes de résolution efficaces

Il s'agit ensuite de proposer des méthodes efficaces pour résoudre, avec une précision suffisante, le problème posé. La résolution dite analytique, où l'on obtient un résultat exact et général, exprimé par une formule compacte, est généralement hors de portée, sauf cas exceptionnels et très simples. Le scientifique ou l'ingénieur doit se contenter d'une résolution numérique — réalisée par ordinateur car les calculs nécessaires sont très volumineux — qui donne le résultat sous forme de valeurs numériques (des nombres), valables avec une certaine approximation. D'importantes difficultés apparaissent ici aussi.

Ainsi, dans les problèmes mettant en jeu la diffraction d'ondes par des objets, le milieu de propagation est souvent illimité : l'onde peut aller jusqu'à l'infini. Or pour que la solution du problème soit unique, il faut imposer une condition dite de rayonnement qui spécifie comment l'amplitude de l'onde décroît au fur et à mesure qu'elle s'éloigne. Cette condition n'est pas simple à imposer numériquement. L'une des solutions proposées consiste à transformer l'équation aux dérivées partielles d'origine en une *équation intégrale* (équation où les fonctions inconnues apparaissent dans des intégrales) ; l'avantage de cette formulation est qu'elle satisfait automatiquement la condition de rayonnement.

C'est dans les années 1960 qu'ont été écrits les premiers programmes informatiques de résolution par équations intégrales. Ils ne permettaient de calculer que la diffraction par des objets petits par rapport à la longueur d'onde ; de plus, ils donnaient souvent des



Un problème typique de propagation d'ondes : une source S émet une onde radar, lumineuse, acoustique ou autre (en rouge sur la figure) de longueur d'onde bien définie ; l'onde se réfléchit partiellement (en bleu et vert sur la figure) sur les deux obstacles présents O_1 et O_2 ; quelle va être l'amplitude de l'onde résultante en chaque lieu, par exemple au niveau d'un détecteur placé en S ? La résolution de ce problème difficile doit prendre en compte le type d'ondes émises, leur longueur d'onde, la forme des obstacles, le matériau dont ceux-ci sont constitués, etc.

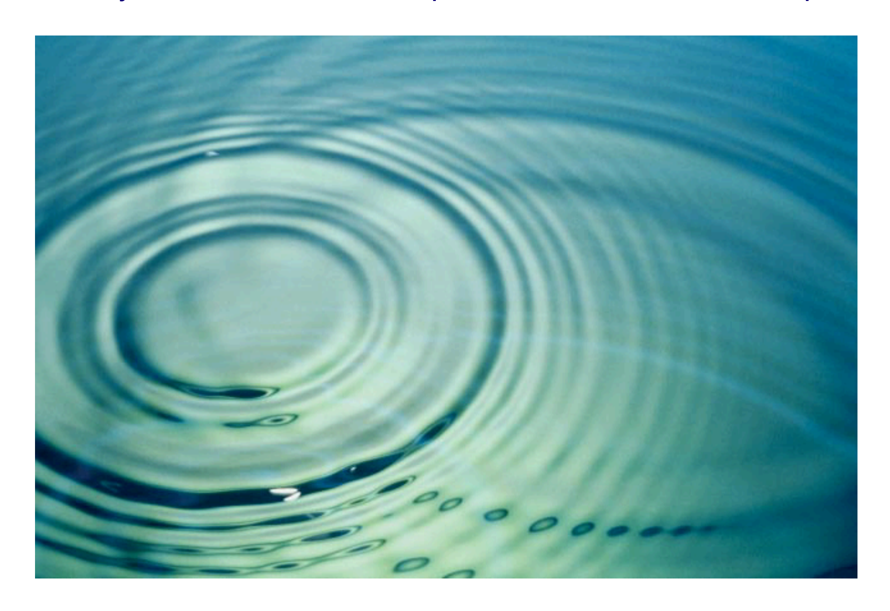


résultats aberrants, faute d'une analyse mathématique suffisante. La compréhension des problèmes rencontrés et leur résolution ont permis, à partir de la fin des années 1980, de calculer avec de plus en plus de précision la diffraction d'une onde par des objets de plus en plus grands par rapport à la longueur d'onde. Les recherches se prolongent aujourd'hui dans divers domaines : choix de la formulation intégrale la mieux adaptée au problème, techniques numériques pour résoudre l'équation. En particulier, les méthodes dites *multipolaires* ont permis d'augmenter notablement la taille des problèmes traitables. Ces travaux ont contribué à la réalisation d'outils logiciels fiables, capables de calculer avec précision le champ ondulatoire diffracté par des objets de taille atteignant plusieurs dizaines de fois la longueur d'onde. C'est, notamment, le cas d'un avion dans le champ d'un radar de longueur d'onde métrique.

Une méthode concurrente de la formulation en équations intégrales consiste à résoudre directement l'équation aux dérivées partielles, et à s'affranchir de la condition de rayonnement en limitant artificiellement le milieu de propagation par une « condition aux limites absorbantes » : on impose (mathématiquement) la présence d'une frontière imaginaire qui absorbe complètement toutes les ondes qu'elle recueille. Ces conditions aux limites absorbantes ont longtemps été responsables de l'apparition, dans les solutions numériques, de phénomènes de réflexions parasites ; ils étaient particulièrement gênants dans le cas d'objets faiblement diffractants. Mais les techniques numériques faisant appel aux conditions aux limites absorbantes ont elles aussi considérablement progressé ; elles offrent à présent un niveau de réflexion parasite très faible, grâce à des travaux théoriques réalisés essentiellement au début des années 1990.

L'optique géométrique et ses généralisations, au service des courtes longueurs d'onde

Lorsque la taille des obstacles qui diffractent les ondes est très grande par rapport à la longueur d'onde (une gouttelette d'eau éclairée par de la lumière visible, un avion balayé par un radar de longueur d'onde décimétrique, etc.), il existe une voie un peu plus facile que la résolution directe des équations des ondes : la bonne vieille optique géométrique. Celle-ci assimile les ondes lumineuses à des rayons qui se propagent en ligne droite dans un milieu donné, et qui sont soumis aux lois simples de la réflexion et de la réfraction découvertes plusieurs siècles avant les équa-



Des ondes se propageant à la surface de l'eau : même ce phénomène quotidien et banal peut être extrêmement difficile à décrire correctement et avec précision. (Photo : Getty Images)



tions décrivant les ondes électromagnétiques. L'un des apports des physiciens, en particulier l'Allemand Arnold Sommerfeld (1868-1951), a été de montrer que l'optique géométrique est en définitive une manière de résoudre les problèmes de diffraction lorsque les objets sont infiniment grands par rapport à la longueur d'onde.

Mais bien sûr, la taille des objets réels n'est pas infinie : l'optique géométrique n'est donc qu'une approximation plus ou moins bonne. Aussi a-t-elle été ensuite étendue et généralisée afin de déterminer le champ ondulatoire aux endroits où l'optique géométrique classique prévoyait uniquement de l'ombre. Ces travaux, entamés dans les années 1950, se poursuivent ; ils permettent de disposer d'outils, certes moins précis que les méthodes de résolution numérique directe d'équations aux dérivées partielles, mais opérants dans le domaine des courtes longueurs d'onde.

Malgré toutes ces avancées, de nombreux problèmes ondulatoires ne sont toujours pas résolus de manière satisfaisante. Il en est ainsi de la diffraction par des objets de grande taille par rapport à la longueur d'onde, mais de forme complexe, avec des détails fins par rapport à la longueur d'onde (cas d'un avion, ou d'un missile, lorsqu'on veut prendre en compte leur forme détaillée au boulon près, et non leur allure générale). Il reste encore beaucoup à faire !

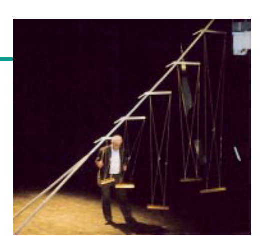
Daniel Bouche
CEA (Commissariat à l'énergie atomique),
Département de physique théorique et appliquée,
Direction d'Île-de-France

Quelques références :

- Site Internet du projet de recherche « Ondes » à l'INRIA : http://www.inria.fr/recherche/equipes/ondes.fr.html
- G. B. Whitham, *Linear and non-linear waves* (Wiley, 1974).
- D. S. Jones, *Acoustic and electromagnetic waves* (Oxford University Press, 1986).
- J. A. Kong, *Electromagnetic wave theory* (Wiley, 1990).
- E. Darve, « The fast multipole method : numerical implementation », *Journal of Computational Physics, 160 (1)*, pp. 195-240 (2000).
- D. Bouche et F. Molinet, *Méthodes asymptotiques en électromagnétisme* (Springer-Verlag, 1994).

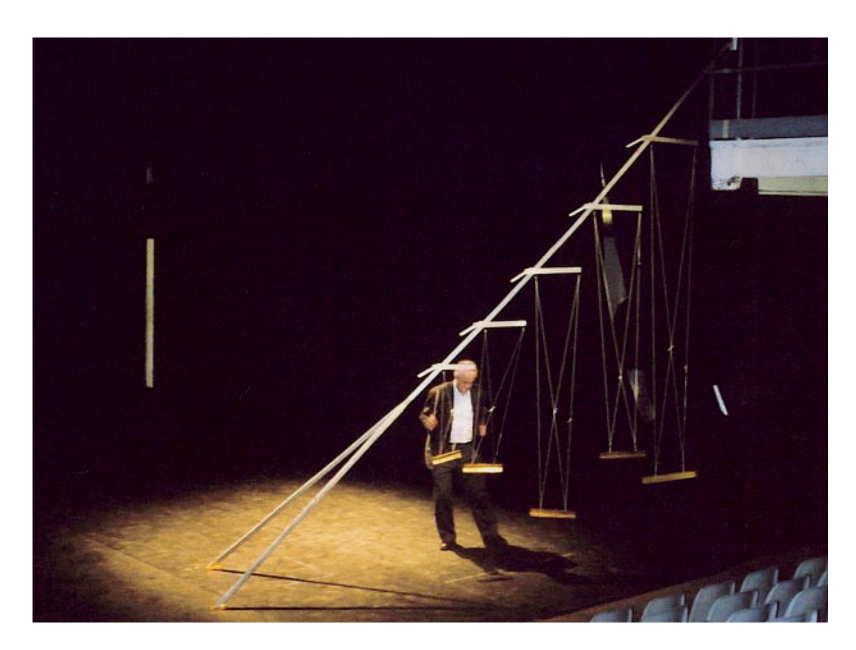
Quand art rime avec maths

Francine Delmer



Les mathématiques n'inspirent pas que les scientifiques. De nombreux artistes y ont puisé la matière de certaines de leurs œuvres. La réciproque est parfois vraie aussi, comme dans le cas de la perspective, où l'art a montré le chemin à des théories géométriques.

De novembre 2000 à janvier 2001, la Galerie nationale du Jeu de Paume présente une rétrospective du plasticien François Morellet, artiste que le critique Thomas McEvilley qualifie, dans le catalogue de l'exposition, de « pythagoricien postmoderne ». En février 2001, Tom Johnson se voit décerner la *Victoire de la musique* de création musicale contemporaine pour sa pièce *Kientzy Loops*. Ce compositeur élabore des transpositions musicales de suites qui agissent comme des contraintes, détourne les automates, décline le triangle de Pascal (*Self-Replicating Loops, Canons rythmiques*, etc.). Il place toujours les concepts mathématiques en préalable à ses œuvres, et poursuit de longue date dialogues et questionnements fructueux avec Jean-Paul Allouche, chercheur en théorie des nombres et informatique théorique. La même année, *Proof* de David Auburn, qui met en scène la vie de mathématiciens, obtient le prix Pulitzer de théâtre. Écrite pour un public néophyte,



On raconte que Galilée aurait observé, dans la cathédrale de Pise, les balancements des lustres pendus à la voûte au lieu d'écouter le sermon. Il eut l'idée de compter les oscillations, remarqua que leurs fréquences étaient différentes mais qu'elles étaient inversement proportionnelles à la racine carrée de la longueur du pendule. C'est sur cette constatation que s'appuie l'œuvre Galileodu compositeur Tom Johnson. Ici, les pendules sont suspendus à une structure dessinée et construite par l'artiste-ingénieur bordelais Eric Castagnès. (Cliché Eric Castagnès)

cette œuvre offre une vision intéressante du travail de chercheur et met en exergue certaines caractéristiques de ce milieu. On peut y déceler des clins d'œil à l'histoire récente et singulière du mathématicien américain John Forbes Nash, des allusions à celle de la démonstration du théorème de Fermat par le chercheur anglais Andrew Wiles.

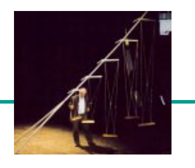
Ces trois événements, relayés par les médias, illustrent l'actualité de la fascination réciproque entre mathématiciens et artistes. Continûment dans l'histoire, leurs relations parcourent l'ensemble des domaines artistiques et s'entretiennent à des niveaux très diversifiés, comme en témoignent philosophes, historiens de l'art, épistémologues, artistes et mathématiciens lorsqu'ils débattent de leur réalité et de leur pertinence. Il ne s'agira pas ici de légitimer quelque création artistique par ses références à des théories scientifiques, ni de porter un jugement de valeur ou de tenter une quelconque classification des pratiques mathématiques et artistiques. Nous nous bornerons seulement à éclairer ces liens d'un regard pointilliste.

Entre les arts et les mathématiques, des liens tissés de tout temps

C'est pour la construction des pyramides dit-on, que les Égyptiens, environ 2 700 ans avant notre ère, utilisaient les triangles sacrés de côtés 3, 4, 5 donnant l'angle droit (ces mesures vérifient la relation « carré de l'hypoténuse = somme des carrés des deux autres côtés » qui caractérise les triangles rectangles). On pense aussi aux théories pythagoriciennes — vers 500 ans avant J.-C. — des rapports numériques qui vont gouverner l'harmonie musicale. Plus près de nous, Albrecht Dürer et Léonard de Vinci, figures emblématiques de l'esprit humaniste de la Renaissance, se sont intéressés à la géométrie, à l'optique, à l'architecture et aux questions tant théoriques que pratiques inhérentes à ces domaines. Dürer, nourri des réflexions et des travaux des Italiens, en particulier Piero della Francesca et Alberti, a fixé dans son traité de géométrie *Underweysung der messung* (1525) les règles de la perspective. Dès lors, les artistes en feront largement usage dans leurs œuvres, tandis que les mathématiciens français Girard Desargues puis Gaspard Monge développeront aux XVIIe et XVIIIe siècles les géométries projective et descriptive. Il faut noter dans ce cas précis la préséance de l'art sur la science : comme l'explique l'historien de l'art Eric Valette, « *l'invention de la perspective est certainement un des plus flagrants exemples où le système symbolique artistique apporte une connaissance du monde encore inconnue pour la science* ».

En littérature, la mathématique pourrait paraître moins présente. Cependant, les membres de l'Oulipo (*Ouvroir de littérature potentielle*, fondé en 1960 par Raymond Queneau et François Le Lionnais, écrivains et mathématiciens), y puisent souvent leurs contraintes d'écriture. Ainsi, dans *La Vie mode d'emploi* de Georges Perec, les ressorts de l'intrigue répondent au problème combinatoire du carré bi-latin orthogonal d'ordre dix.

Au XXe siècle, la création musicale a été marquée par les compositeurs Pierre Boulez et Iannis Xenakis, tous deux formés aux mathématiques. Boulez développe dans ses compositions les principes du sérialisme, tandis que Xenakis fait appel à un contrôle statistique des paramètres musicaux dans sa musique stochastique, pour ne citer qu'un exemple dans le foisonnement de leur création. L'IRCAM créé en 1970 par Pierre Boulez et au sein duquel travaillent nombre de



musiciens, acousticiens, mathématiciens et informaticiens — aux formations mixtes — atteste encore de l'imbrication profonde des mathématiques et de la musique en ce début du XXIe siècle, tant au niveau technique que théorique. Une intéressante mise en perspective des questions relatives à ce sujet y fut présentée au cours du Quatrième forum mathématique Diderot organisé en décembre 1999 par la Société européenne de mathématiques, sous le titre Logiques mathématiques, *logiques musicales au XXe siècle.*

Les mathématiques, tantôt simple outil, tantôt moteur théorique de la création

Ces quelques échantillons illustrent la diversité des relations entre mathématiques et arts et posent quelques questions. Les mathématiques sont-elles utilisées, par tel art, pour des raisons techniques ou théoriques ? Inspirent-elles les artistes de façon métaphorique ou symbolique ?

Le peintre François Morellet, déjà cité, utilise au plus près l'outil mathématique ; en témoignent ses œuvres *Répartition aléatoire de quarante mille carrés suivant les chiffres pairs et impairs d'un annuaire de téléphone*, *π ironicon n° 2*, etc., où il suggère l'idée de l'infini. Selon le critique d'art Gilles Gheerbrandt, « *chez lui, les mathématiques (élémentaires) peuvent servir à la formulation des problèmes, mais elles sont un simple outil, jamais une fin en soi* ». L'artiste, de son côté, affirme utiliser les mathématiques pour échapper à toute subjectivité ou affectivité, pour garder une distance vis-à-vis de l'œuvre, pour la désensibiliser ; il renoue ainsi avec la vieille idéologie platonicienne



L'artiste François Morellet, un « pythagoricien postmoderne ». (Cliché Gamma/Raphaël Gaillarde)

consistant à dénoncer les charmes de l'art qui ne seraient que tromperie.

Si certains artistes usent de notions élémentaires comme références ou prétextes, d'autres s'approprient les principes de théories mathématiques dans leurs fondements, puisant alors à l'essence du raisonnement. Le peintre Albert Aymé, l'un des exemples les plus radicaux de plongée dans l'abstraction, s'appuie sur une démarche analogue à celle de la recherche mathématique. Rejetant les mécanismes combinatoires, il développe sa réflexion dans des traités — *Approche d'un langage spécifique, Sur les paradigmes*, etc. — qui donnent le cadre de son projet pictural : « *Je m'efforce d'avancer dans mon travail avec la rigueur d'un scientifique mais sans me dissocier pour autant de la passion du poète ou du musicien* ». L'œuvre, au demeurant, peut se passer du discours et reste « intrinsèquement belle », l'art abstrait n'étant, à son sens, « *pas une affaire de goût mais de méthode* ».

Activités humaines, les mathématiques et les arts sont le fait d'individus plongés dans le même climat culturel, politique, religieux. Les grandes ruptures de l'histoire ne laissent aucun de ces domaines sur le bord du chemin en raison d'interactions qui semblent tributaires de l'esprit du temps. N'est-ce pas, en effet, à la lecture des écrits philosophiques de Henri Poincaré, qui popularise au tournant du XXe siècle les idées de la géométrie non euclidienne, que les cubistes balayent la perspective traditionnelle ?

Soyons en conscients, toute volonté de fusion ou d'unification entre mathématiques et arts serait réductrice et vaine. C'est bien la connaissance et la curiosité qui permettent échanges et confrontations dans un abord propre à chaque forme d'expression. Constatons seulement avec bonheur que les mathématiques et les arts jouent ensemble, encore et toujours, une partition de lumière.

Francine Delmer
Laboratoire Arithmétique et Algorithmique expérimentale
Université Bordeaux 1, Talence

Quelques références :

- E. Valette, *La perspective à l'ordre du jour* (L'Harmattan, 2000).
- G. Gheerbrant, « François Morellet », *Parachute*, Montréal, n° 10, p. 5 (printemps 1978).
- M. Loi (sous la dir. de), *Mathématiques et arts* (Hermann, 1995).
- J.-L. Binet, J. Bernard, M. Bessis (sous la dir. de), *La création vagabonde* (Hermann, collection Savoir, 1980).
- V. Hugo, *L'art et la science* (Anaïs et Actes Sud, 1864/1995).
- M. Sicard (sous la dir. de), *Chercheurs ou artistes* (Autrement, série Mutations, n° 158, 1995).
- I. Xenakis, *Arts/sciences. Alliages* (Casterman, 1979).
- J.-M. Lévy-Leblond, *La pierre de touche - la science à l'épreuve* (Gallimard, 1996).
- J. Mandelbrot, « Les cheveux de la réalité - autoportraits de l'art et de la science », *Alliage*, 1991.
- D. Boeno, « De l'usage des sections coniques », *Cahiers art et science, n° 5*, pp. 41-54 (Confluences, 1998).



Centre National d'Etudes Spatiales
CNES

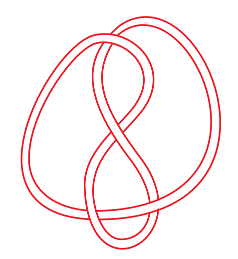
Chargé du développement des activités spatiales françaises depuis 1961, le CNES a pour mission de proposer au gouvernement les orientations de la politique spatiale de la France et de mettre en œuvre, avec le concours de ses partenaires (industriels, entités de recherche, organismes de défense), les programmes décidés.

Le CNES intervient dans des domaines aussi variés que l'observation de la Terre, les télécommunications, les sciences de l'univers, la présence de l'homme dans l'espace, et assure depuis 1973, par délégation de l'Agence spatiale européenne (ESA), la responsabilité de maîtrise d'œuvre du programme Ariane.

Le CNES réunit 2500 agents répartis sur 5 sites différents.

Centre National d'Etudes Spatiales
2 place Maurice Quentin
75039 Paris Cedex 01
Tél. : 01.44.76.75.00
www.cnes.fr et www.cnes-tv.net

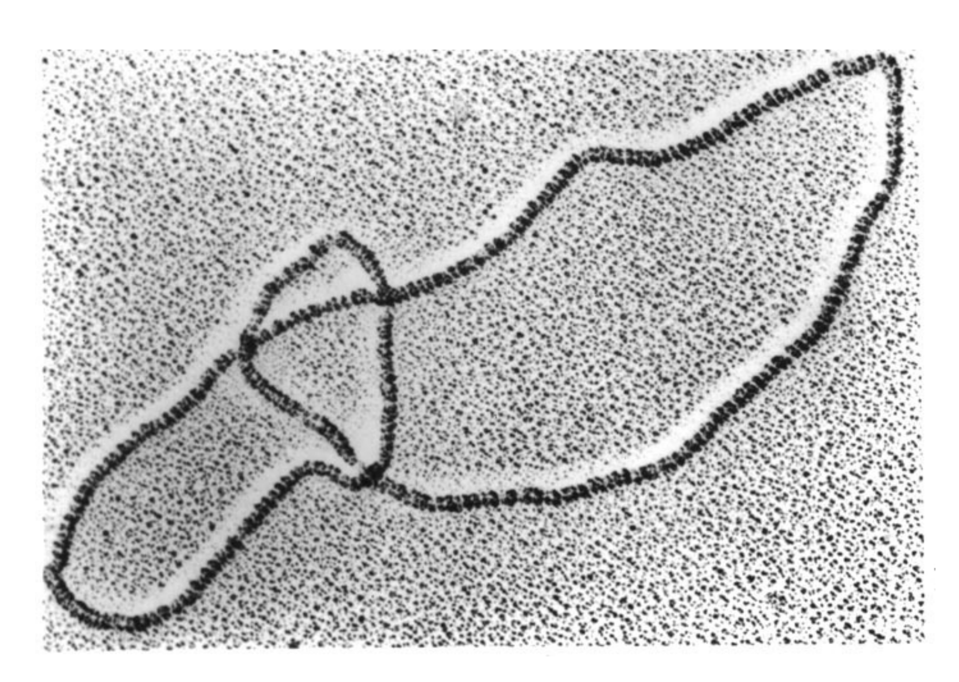
De l'ADN à la théorie des nœuds



Nguyen Cam Chi et Hoang Ngoc Minh

L'activité biologique de la molécule d'ADN dépend notamment de son agencement dans l'espace et de la façon dont elle est entortillée — choses qui sont du ressort de la théorie mathématique des nœuds.

Personne aujourd'hui ne peut l'ignorer : l'ADN est la molécule qui, dans chaque cellule des êtres vivants, porte l'information génétique et commande pour une large part l'activité cellulaire. L'ADN comporte en général deux longs brins parallèles constitués d'un enchaînement de molécules appelées bases nucléotidiques, les deux brins tournant l'un autour de l'autre en formant une structure hélicoïdale : la célèbre double hélice.



Une molécule d'ADN circulaire et nouée, vue au microscope électronique. La topologie de la molécule d'ADN influence son activité. (Cliché N. Cozzarelli, université de Berkeley)

L'information portée par l'ADN est codée par la séquence de paires de bases nucléotidiques. Cette séquence ne dépend pas de la façon dont la molécule est tortillée, mêlée ou nouée. Dans les années 1960-1970, cependant, après la découverte des molécules d'ADN circulaires (des boucles composées d'un seul brin ou de deux brins enroulés l'un autour de l'autre), on a commencé à s'interroger sur l'influence de la forme topologique de l'ADN,

c'est-à-dire sa disposition dans l'espace. En 1971, le biochimiste américain James Wang a mis en évidence que certaines enzymes, les topo-isomérases, peuvent modifier la configuration topologique de l'ADN, par exemple en y créant des nœuds, et que la topologie de la molécule d'ADN influe sur son fonctionnement dans la cellule. L'étude des configurations topologiques de l'ADN peut donc nous renseigner sur la façon dont l'ADN intervient dans les mécanismes cellulaires.

La topologie, que certains définissent comme la « géométrie du caoutchouc » — c'est-à-dire l'étude de propriétés qui ne sont pas modifiées par une déformation, par une modification des longueurs — est une branche importante et fondamentale des mathématiques. Ses concepts et méthodes sont nécessaires à quasiment tous les mathématiciens. La théorie des nœuds en est une émanation particulière. Née il y a environ un siècle, celle-ci vise à étudier précisément la structure des nœuds, et à les classer. Elle a trouvé des applications dans d'autres disciplines scientifiques (en chimie moléculaire, en physique statistique, en physique théorique des particules, etc.), en plus de ses liens avec d'autres domaines de la recherche mathématique.

La question fondamentale de la théorie des nœuds est la suivante : étant donnés deux nœuds (pas trop simples !) réalisés par exemple avec du fil, peut-on dire s'ils sont équivalents ? En d'autres termes, peut-on étirer ou déformer l'un pour le rendre identique à l'autre, sans rien couper ? Comme les topologues s'autorisent des déformations, leur définition d'un nœud est légèrement différente de celle de l'homme de la rue : pour eux, un nœud s'obtient en joignant les deux extrémités du fil ; sinon, on pourrait — en tirant et en déformant convenablement le fil — dénouer n'importe quel nœud, et tous les nœuds seraient alors équivalents. Du point de vue de la topologie, donc, un nœud est obligatoirement constitué d'une ou plusieurs boucles — ce qui est le cas des ADN circulaires.

Classer les nœuds en recherchant des « invariants » : un problème de topologie algébrique

Les spécialistes des nœuds font en général de la *topologie algébrique* : ils cherchent à associer à chaque nœud topologiquement différent un « invariant », un objet mathématique qui le caractérise, calculable aisément et qui se prête à des manipulations algébriques. Cet objet mathématique peut être, *a priori*, un nombre, un polynôme (une expression algébrique comme $x^6 - 3x^2 + x + 2$) ou quelque chose de plus compliqué ou abstrait. L'important, c'est qu'il soit le même pour tous les nœuds topologiquement équivalents (d'où le terme d'invariant). L'idéal est de trouver des invariants qui caractérisent complètement les nœuds, c'est-à-dire tels que deux nœuds distincts aient forcément des invariants différents. Alors le problème de classification sera résolu. Pour résumer, les principales questions sont : a-t-on une manière de caractériser les nœuds afin de les distinguer ? Existe-t-il un algorithme pour distinguer deux nœuds ? Existe-t-il un programme informatique permettant à un ordinateur de distinguer deux nœuds donnés en un temps raisonnable ?

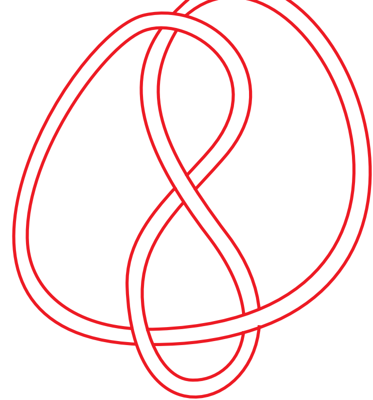
Malgré plusieurs décennies de recherches, la réponse à ces questions reste incomplète. D'importants progrès ont toutefois été réalisés. Évoquons en quelques-uns, brièvement. En 1928, le mathématicien américain James Alexander a introduit le premier invariant poly-

nomial (le polynôme d'Alexander) permettant de classer des nœuds. Mais le polynôme d'Alexander est un invariant incomplet : certains nœuds distincts ont le même polynôme d'Alexander. Beaucoup plus récemment, en 1984, le mathématicien néo-zélandais Vaughan Jones a découvert un nouvel invariant, lui aussi polynomial ; il est plus efficace que le polynôme d'Alexander, mais lui non plus ne résout pas entièrement le problème de classification. Quelque temps après, d'autres chercheurs ont affiné et généralisé l'invariant de Jones ; là encore, les nouveaux invariants polynomiaux introduits sont incomplets et échouent à faire la différence entre certains nœuds topologiquement distincts.

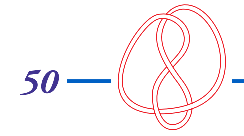
Un début de solution complète est peut-être intervenu vers 1990, avec les travaux du chercheur moscovite Victor Vassiliev. Ce dernier a introduit une nouvelle classe d'invariants définis de manière implicite, c'est-à-dire définis seulement par les relations qu'ils doivent vérifier entre eux. Les invariants de Vassiliev sont numériques, c'est-à-dire qu'à chaque nœud est associé un nombre (qui peut être déterminé à partir d'une analyse combinatoire de la topologie du nœud). Vassiliev a conjecturé que ces invariants forment un système complet, autrement dit que des nœuds distincts ont toujours des invariants de Vassiliev différents. Bien qu'aucun contre-exemple n'ait été trouvé jusqu'à présent, la conjecture reste à prouver, de même qu'il reste à trouver des méthodes pour calculer de façon effective et efficace les invariants de Vassiliev. Tout de même, l'avancée est considérable.

Un parallèle existe entre des transformations mathématiques et des mécanismes enzymatiques

Ces recherches mathématiques ont des liens avec les questions que se posent les biologistes à propos de molécules comme l'ADN. Par exemple, vers 1973, le mathématicien britannique John Conway a introduit des opérations « chirurgicales » élémentaires (le flip et le décroisement) qui permettent de transformer un nœud en un autre en modifiant le nœud au niveau d'un croisement de ses brins. Or ces opérations de nature mathématique ont des équivalents biochimiques, réalisés par des topo-isomérases. Ces enzymes, indispensables au fonctionnement de toutes les cellules, peuvent couper d'abord l'un des brins ou les deux brins de l'anneau d'ADN circulaire et passer un segment de l'anneau à travers l'ouverture, et refermer ensuite les extrémités coupées pour faire un nœud dans chaque anneau. En effectuant les opérations de coupure, de passage et



Les deux nœuds représentés ici sont topologiquement distincts : on ne peut passer de l'un à l'autre en tirant seulement les fils, sans couper et recoller. Le nœud de gauche (nœud de trèfle) a pour polynôme d'Alexander le polynôme $P(t) = t^2 - t + 1$; celui de droite a pour polynôme d'Alexander $P(t) = t^2 - 3t + 1$. Comme il se doit, ces deux polynômes sont distincts. Cependant, il existe des nœuds distincts associés à un même polynôme d'Alexander : les polynômes d'Alexander ne constituent pas des invariants complets.



de ressoudage, elles peuvent couper un brin, faire passer l'autre brin par l'ouverture obtenue puis ressouder cette coupure (cela correspond à l'opération *flip* de Conway), ou bien effectuer deux coupures, deux ressoudages en attachant les deux brins « à l'envers » (opération *décroisement* de Conway).

Maintenant, comment la topologie de l'ADN peut-elle influencer son activité biologique ? Illustrons-le sur l'exemple du surenroulement de la molécule d'ADN. Dans son état habituel, les brins de la double hélice moléculaire décrivent un certain nombre de tours autour de l'axe de l'hélice. Certaines topo-isomérases peuvent augmenter ou réduire cet entortillement, un peu comme on peut surenrouler ou sous-enrouler un fil de téléphone, ce qui modifie sa forme. Qui plus est, dans un ADN circulaire, le nombre de tours de la double hélice est une propriété topologique invariante : il ne peut être changé par aucune modification de la forme de la structure, sauf celle qui implique la coupure et la reconstruction des brins de l'anneau de l'ADN bicaténaire. Or si un anneau d'ADN est désenroulé, on voit aisément que la double hélice devient moins compacte, et que sa partie interne devient plus exposée à l'action des enzymes qui l'entourent. Une telle exposition préconditionne la réplication (formation d'un deuxième exemplaire de la molécule) de l'ADN et sa transcription (processus qui conduit la cellule à synthétiser des protéines).

La configuration topologique de l'ADN étant déterminée par un mécanisme enzymatique, une des questions légitimes pour les biologistes est de savoir dans quelle mesure une classification topologique des nœuds permet de remonter aux mécanismes enzymatiques à l'œuvre. Une autre question voisine est de savoir si l'on peut simuler tous ces mécanismes enzymatiques en utilisant les opérations de base introduites pour les nœuds mathématiques. Les recherches aux frontières entre mathématiques des nœuds et biologie moléculaire sont loin d'être épuisées.

Nguyen Cam Chi et Hoang Ngoc Minh
Département de mathématiques et d'informatique,
Université de Lille 2

Quelques références :

- « La science des nœuds », dossier hors-série de *Pour la Science*, avril 1997.
- A. Sossinsky, *Nœuds - Genèse d'une théorie mathématique* (Seuil, 1999).
- D. W. Sumners, « Lifting the curtain : using topology to prob the hidden action of enzymes », *Notices of the American Mathematical Society, 42 (5)*, pp. 528-537 (mai 1995).

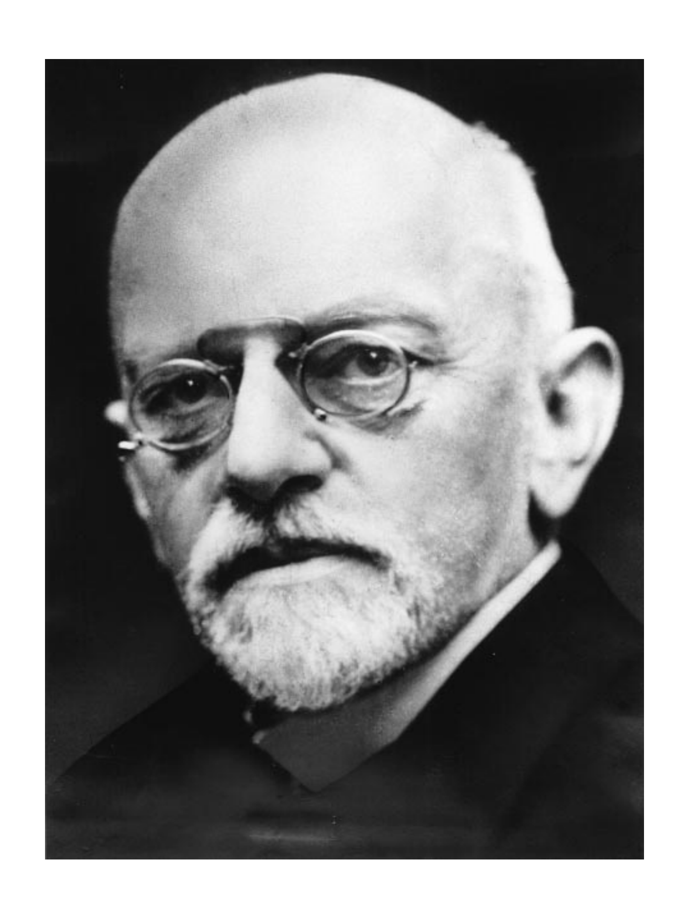
Le philosophe et le mathématicien



Pierre Cassou-Noguès

Tout au long de leur histoire, la philosophie et les mathématiques ont entretenu une relation aussi étroite qu'énigmatique. Il faudrait revenir à Platon dans le monde grec et à Descartes à l'aube de l'époque moderne. Évoquons ici deux grandes figures du XXe siècle, David Hilbert et Edmund Husserl.

Edmund Husserl et David Hilbert se rencontrent à Göttingen en 1901. Le philosophe, Husserl, a suivi des études de mathématiques. Il a été à Berlin l'assistant de Karl Weierstrass, grand mathématicien analyste, avant de rencontrer Franz Brentano, à Vienne, et de se tourner vers la philosophie. Il a publié en 1891 la *Philosophie de l'arithmétique*. Le premier tome de ses *Recherches logiques* paraît en même temps que le philosophe s'installe à Göttingen. Le mathématicien, Hilbert, est à Göttingen depuis 1897. Il a résolu un problème fameux, le « problème de Gordan », en théorie des invariants, qui, depuis une vingtaine d'années, préoccupait les géomètres allemands. Il a développé, en algèbre, la « théorie des corps algébriques ». Husserl et Hilbert ont à peu près le même âge. Ils se croisent à la Faculté de philosophie qui regroupe, en réalité, les philosophes et les mathématiciens. Ils vont, l'un comme l'autre, transformer leur discipline. Husserl découvre la phénoménologie. Hilbert met en place la méthode abstraite qui caractérise les mathématiques modernes.



David Hilbert (1862-1943) était, avec le Français Henri Poincaré, l'un des grands mathématiciens des années 1900. Par la profondeur de ses travaux et de ses points de vue, par le dynamisme qu'il a su insuffler à Göttingen, il a exercé une influence considérable sur les mathématiques du XXe siècle. (Cliché AKG)



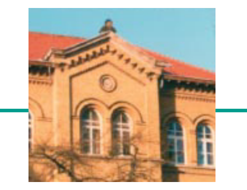
Göttingen, lieu d'excellence mathématique, accueille les philosophes

Si Göttingen n'était qu'une petite ville, près de Stuttgart, elle devient, peu après 1900, le centre du monde mathématique. Felix Klein est à la tête de la Faculté. Ce grand géomètre, qui a établi de façon définitive l'existence des espaces non euclidiens, renonce à la recherche et se consacre à ses cours, sur le développement des mathématiques au XIXe siècle, et à l'administration de la Faculté, pour laquelle il réunit de nouveaux moyens financiers. Il fait venir Hilbert puis Hermann Minkowski. Ce dernier introduira, lors d'une leçon célèbre, le « continuum d'espace-temps » — qui porte son nom et qui servira de cadre à Einstein pour formuler la théorie de la relativité. Chaque semaine, la Société mathématique de Göttingen se réunit autour d'un conférencier, de Göttingen ou d'ailleurs. Husserl, le philosophe, parle en avril 1901 du problème des imaginaires en arithmétique. Göttingen est un lieu consacré aux mathématiques. On raconte qu'un jour Minkowski, se promenant dans la rue principale, vit un jeune homme pensif, en proie à quelque tourment ; il lui tapa gentiment sur l'épaule et lui dit : « ne vous inquiétez pas, ça converge », sur quoi le jeune homme s'éloigna, rassuré.

C'est à Göttingen que Hilbert mûrit la méthode abstraite des mathématiques modernes. La méthode abstraite est née dans l'algèbre du XIXe siècle. Richard Dedekind et Leopold Kronecker, notamment, ont introduit ce qu'on appelle des structures. On définit une structure mathématique, comme celle de « groupe », d'« espace vectoriel », de « corps »,



Un des bâtiments de mathématiques (l'Institut de mathématiques appliquées et numériques) de l'université de Göttingen, aujourd'hui. Entre 1900 et 1930, Göttingen a été pour les mathématiques un centre de renommée mondiale, grâce aux efforts de David Hilbert. Les mathématiciens y cotoyaient des philosophes et des scientifiques d'autres disciplines. (Cliché université de Göttingen)



en fixant les règles que vérifient les opérations, sans considérer la nature des objets soumis à ces opérations. Ainsi, une même structure peut s'appliquer à des objets de nature différente — à des nombres, à des fonctions, à des transformations géométriques, etc. L'abstraction, en mathématiques, consiste à se détourner, ou à faire abstraction, de la nature des objets pour ne considérer que les relations qu'entretiennent ces objets. Ce point de vue, qui émerge dans l'algèbre de Dedekind et qui est resté anonyme au XIXe siècle, Hilbert le rend explicite.

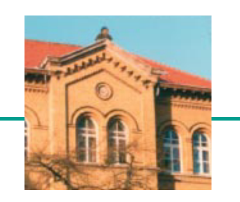
Hilbert donne une représentation axiomatique de la géométrie

Dès son arrivée à Göttingen, Hilbert annonce un cours sur la géométrie. Ce cours, qui sera publié sous le titre *Les fondements de la géométrie*, s'appuie sur la méthode abstraite pour donner une axiomatisation de la géométrie. Hilbert fait abstraction de la nature des objets géométriques, le point, la droite, le plan, et se contente de poser entre eux des relations dont les propriétés sont explicitées par les axiomes. Autrement dit, les axiomes fixent les propriétés des relations existant entre des objets dont la nature est laissée indéterminée. Ainsi, les axiomes définissent une structure, analogue aux structures algébriques. Mais, de l'algèbre à la géométrie, le primat de la structure est renforcé. En algèbre, on donne une structure à des objets supposés connus, des nombres, des fonctions. On peut déduire un théorème en raisonnant à partir de la structure ou bien en raisonnant sur les objets, avec leur nature propre. En revanche, par axiomatisation, le raisonnement est réduit à une simple déduction à partir des axiomes et les objets sont définis par la seule position des axiomes. Les axiomes, c'est-à-dire la structure, suffisent à définir les objets et à effectuer des démonstrations sur ces objets.

Dans son axiomatisation de la géométrie et dans ses travaux ultérieurs, Hilbert explicite la méthode abstraite de l'algèbre, la radicalise et l'utilise pour produire de nouveaux résultats. En réalité, Hilbert parcourt et transforme, dans une perspective abstraite, toutes les mathématiques de son temps : la géométrie ; l'algèbre et la théorie des nombres, avec une première démonstration de la « conjecture de Waring » en 1909 ; l'analyse, où il introduit les espaces de Hilbert, espaces abstraits dont les « points » sont par exemple des fonctions. La méthode abstraite sera reprise, à Göttingen, par l'école d'Emmy Noether et d'Emil Artin, puis, en France, par le groupe Bourbaki. Elle nourrira dès lors toutes les mathématiques.

Donner un fondement aux mathématiques

Parallèlement, Hilbert développe la méthode abstraite pour lancer un programme de fondement des mathématiques. Fonder les mathématiques, c'est donner à leurs raisonnements une garantie ultime. Il s'agit en particulier de justifier les raisonnements qui supposent un infini existant en acte, les raisonnements *transfinis*, tout en faisant l'économie de l'hypothèse de l'existence de l'infini. Le programme *formaliste* comporte deux étapes. La première tâche est de formaliser les théories mathématiques. On considère un alphabet de symboles. On fixe des règles, analogues à l'orthographe et à la grammaire, pour construire une formule à partir de ces symboles. On explicite des axiomes, qui serviront

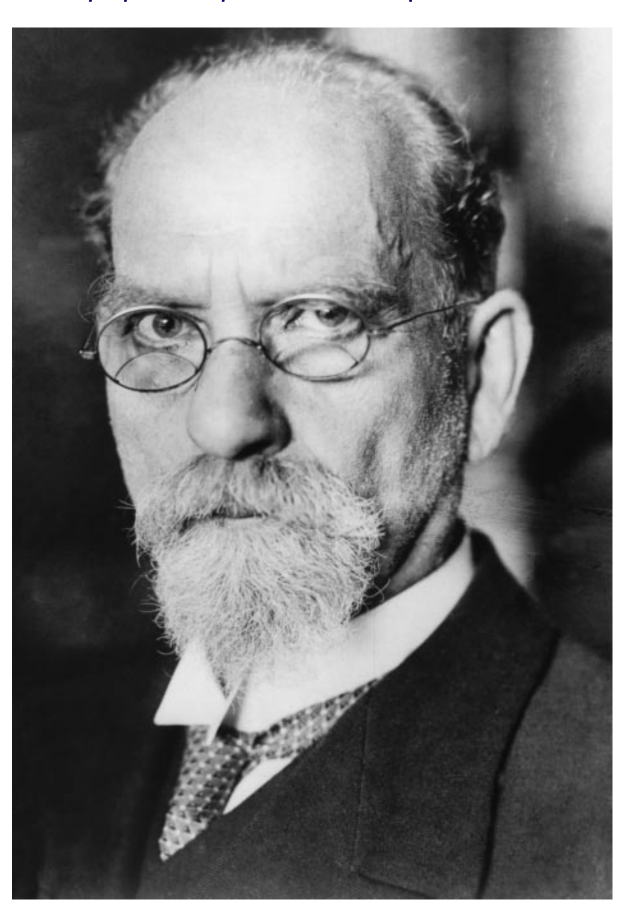


de prémisses dans les démonstrations, et des règles pour déduire une formule d'une autre. Les mathématiques sont remplacées par un stock de formules. Une démonstration consiste en manipulations de symboles selon des règles explicites, abstraction faite du sens des symboles. Une démonstration se présente comme un assemblage de symboles conforme à des règles explicites, un dessin construit selon les règles qu'on s'est fixé. La seconde tâche est de démontrer la non-contradiction de ces systèmes formels au moyen de raisonnements finitistes, c'est-à-dire ne faisant pas intervenir l'infini actuel.

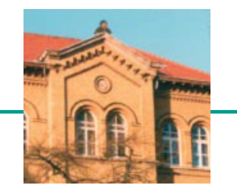
La première théorie à laquelle Hilbert tente d'appliquer ce programme est l'arithmétique, qui comporte déjà des raisonnements transfinis. Ainsi, Hilbert ouvre une *théorie de la démonstration*, qui consiste en raisonnements finitistes portant sur les dessins qui représentent les démonstrations dans un système formel. Toutefois, en 1931, le logicien autrichien Kurt Gödel établit qu'il est impossible de prouver, au moyen de raisonnements finitistes, la non-contradiction d'un système formel incluant l'arithmétique élémentaire. Il faut donc renoncer au programme initial de Hilbert.

La méthode abstraite et le programme formaliste ont fasciné les philosophes

Il reste que Hilbert a réussi à transformer une question philosophique, celle du fondement, en un problème mathématique, traité au moyen de la méthode abstraite et relevant d'une nouvelle théorie, la théorie de la démonstration, qui reste aujourd'hui encore vivante. En retour, la méthode abstraite et le programme formaliste qu'elle sous-tend ont exercé une sorte de fascination sur les philosophes. D'emblée, dans ses *Recherches logiques* de 1901, puis dans *Logique formelle et logique transcendantale* de 1929, Husserl intègre la représentation abstraite des mathématiques à la phénoménologie naissante. Husserl distingue deux mathématiques, une mathématique appliquée, qui comprend par exemple la géométrie en tant que théorie de notre espace, l'espace dans lequel nous vivons, et une mathématique formelle. Partant d'une théorie appliquée, un mathématicien en dégage l'architecture et isole un système d'axiomes, qu'il peut ensuite faire varier pour obtenir de nouvelles formes pour des théories possibles. Ainsi, la mathématique formelle apparaît comme une théorie des formes de théories ou, dans le vocabulaire de Husserl, une *apophantique formelle*, qui vise à définir



Edmund Husserl (1859-1938), qui s'est en partie inspiré de problématiques mathématiques pour édifier sa philosophie. (Cliché AKG)



et à classer tous les systèmes possibles de jugements. En outre, comme l'avait montré Hilbert, procéder de façon axiomatique revient à faire abstraction de la nature des objets. Par conséquent, à chaque forme de théories, correspond un domaine d'objets, d'objets quelconques déterminés par ceci seul qu'ils sont soumis à tel système d'axiomes. La théorie des formes de théories représente donc une *ontologie formelle*, une théorie du pur « quelque chose », qui vise à définir et classer, par leur seule forme, toutes les multiplicités possibles d'objets. La mathématique formelle comporte une double orientation : elle est apophantique formelle, lorsque le mathématicien se tourne vers les systèmes de jugements ; elle est ontologie formelle, lorsque le mathématicien se tourne vers les domaines d'objets. Si Husserl, qui avait étudié de près la géométrie du XIX[e] siècle, disposait des concepts de forme de théories et de multiplicité formelle avant 1901, il est certain que la rencontre avec Hilbert et les discussions à la Société mathématique de Göttingen ont joué un rôle décisif dans l'élaboration d'une phénoménologie systématique.

Hilbert a réussi à poser à l'intérieur des mathématiques la question du fondement des mathématiques. C'est l'intériorisation dans les mathématiques d'une question philosophique. Husserl a opéré l'intériorisation inverse, de la méthode abstraite des mathématiques dans la philosophie. Le parcours de deux hommes, le philosophe Husserl et le mathématicien Hilbert, témoigne d'une intériorisation, réciproque et concomitante, des mathématiques dans la philosophie et de la philosophie dans les mathématiques.

Pierre Cassou-Noguès
CNRS, Laboratoire Savoirs et Textes,
Université Lille III

Quelques références :

- P. Cassou-Noguès, *Hilbert* (Les Belles Lettres, 2001).
- P. Cassou-Noguès, *De l'expérience mathématique. Essai sur la philosophie des sciences de Jean Cavaillès* (Vrin, 2001).
- J.-T. Desanti, *La philosophie silencieuse* (Seuil, 1975).
- D. Hilbert, *Gesammelte Abhandlungen* (Springer, Berlin, 1931-35).
- E. Husserl, *Recherches logiques* (tr. fr. H. Elie, A. L. Kelkel et R. Schérer, P. U. F., 1959).
- C. Reid, *Hilbert* (Springer, 1970).
- H. Sinaceur, *Corps et modèles* (Vrin, 1991).

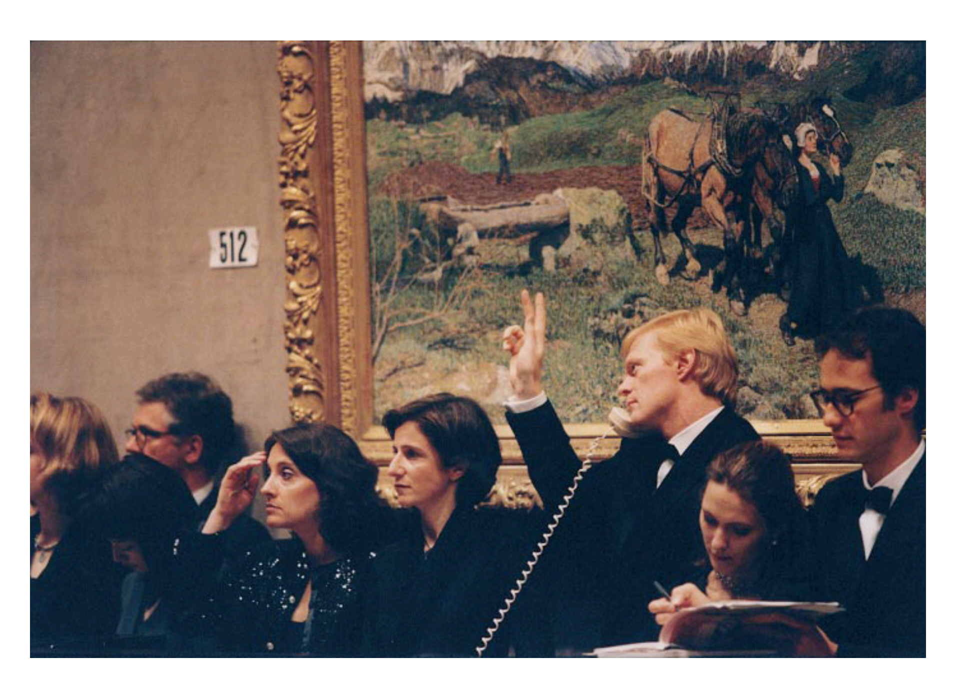
Comment rationaliser les ventes aux enchères ?



Jean-Jacques Laffont

Grâce notamment à Internet, les ventes aux enchères se généralisent. La modélisation de ces procédés de vente permet de définir les règles et stratégies optimales de leur utilisation.

Les enchères constituent un mode d'achat et de vente de plus en plus répandu. C'est en particulier le cas sur Internet, comme en témoigne le succès foudroyant du site eBay où des biens de toutes sortes — des livres aux voitures, en passant par des objets d'art ou des appareils électroménagers — sont mis aux enchères. Méthode d'allocation des ressources rares, les enchères sont traditionnelles dans les marchés de produits de l'élevage et de l'agriculture (poissons, fleurs, etc.). Elles ont été étendues récemment à des biens plus coûteux, comme les appartements, et à des objets beaucoup plus complexes, comme les licences pour la téléphonie mobile de troisième génération.



Une vente aux enchères d'œuvres d'artistes du XXe siècle chez Christie's. Chaque acquéreur potentiel se comporte en fonction de ce qu'il croit que les autres vont faire. La théorie des jeux analyse de telles situations et aide à trouver les stratégies optimales (Cliché Gamma Liaison/Jonathan Elderfield)

L'utilisation du système des enchères est très ancienne, et remonte à l'Antiquité. Ainsi, Hérodote décrit le marché du mariage de Babylone comme une enchère au premier prix (c'est-à-dire que l'offre la plus élevée remporte l'« objet » à vendre), qui démarrait avec les plus belles jeunes femmes.



En Asie, le récit le plus ancien d'enchères concerne la vente des effets des moines décédés, au VIIe siècle.

Les premières conceptualisations des enchères étaient inadaptées, car trop simplistes

Si les enchères remontent presque à l'aube de l'humanité, leur conceptualisation est, elle, beaucoup plus récente. La première œuvre académique importante consacrée à ce sujet est une thèse de 1955, dont l'auteur était l'Américain L. Friedman. C'était l'une des premières thèses de recherche opérationnelle. Elle portait sur le développement des stratégies d'enchère par les entreprises à l'occasion de la vente des droits de forage pétroliers dans le Golfe du Mexique. Il s'agissait d'enchères « au premier prix sous pli fermé » : dans cette procédure, les offres ne sont pas rendues publiques et c'est l'offre la plus élevée qui remporte les enchères.

La démarche adoptée par Friedman consistait simplement à rendre maximale ce qu'on appelle l'espérance de profit. En cas de succès, l'enchérisseur gagne la différence ($v - b$) entre son évaluation v de l'objet mis en vente et le prix b qu'il propose de payer. L'espérance de gain est donc cette différence multipliée par la probabilité $P(b)$ de remporter l'enchère avec un tel prix, soit $(v - b)P(b)$. La probabilité $P(b)$ est *a priori* inconnue ; mais en réalisant une analyse statistique des enchères passées, on découvre les façons d'enchérir des concurrents ; cela permet de déterminer une approximation de la fonction $P(b)$, et par suite de trouver l'enchère b^* qui maximise l'espérance de gain, c'est-à-dire telle que $(v - b^*)P(b^*)$ soit maximal.

Cette méthode, largement utilisée et raffinée de multiples façons, est toutefois extrêmement naïve. En effet, elle suppose implicitement que les autres enchérisseurs n'élaborent pas de stratégies et que leur comportement futur peut être aisément déduit de leur comportement passé. En 1961, le



La page d'accueil du site d'enchères sur Internet eBay-France.

Canadien William Vickrey (qui a reçu le prix Nobel d'économie en 1996, deux jours avant son décès) a posé le problème différemment, en faisant appel à la théorie des jeux.

La théorie des jeux et l'économie mathématique entrent en action pour définir des stratégies optimales

Créée par le célèbre mathématicien d'origine hongroise John von Neumann dans les années 1920-1940, en collaboration avec l'économiste d'origine autrichienne Oskar Morgenstern, la théorie des jeux examine l'interaction d'acteurs stratégiques. Elle concerne toute situation où des acteurs doivent chacun prendre des décisions, qui déterminent l'issue de cette situation. La théorie des jeux s'applique ainsi à de nombreux scénarios de l'univers économique, politique, diplomatique ou militaire. Mais revenons à nos enchères. Lorsqu'un enchérisseur doit décider de sa mise, il s'interroge sur le comportement de ses concurrents, et chaque enchérisseur fait de même. Un *équilibre* de cette situation désigne, pour les spécialistes, un objet assez complexe : c'est une méthode de miser — autrement dit une relation entre l'évaluation v de l'enchérisseur et sa mise b — qui est, pour cet enchérisseur, la meilleure façon de miser compte tenu de ce qu'il anticipe sur la façon de miser des autres acteurs et des croyances qu'il a sur leurs propres évaluations. Par exemple, dans une situation symétrique où les croyances des uns sur les autres sont les mêmes, la stratégie d'un enchérisseur doit maximiser son espérance de profit sachant que tous les autres utilisent la même stratégie que lui.

Le concept que l'on vient d'évoquer est une généralisation de l'*équilibre de Nash*, adaptée au contexte d'information incomplète des enchères. De quoi s'agit-il ? Le mathématicien américain John Nash (prix Nobel d'économie en 1994) avait proposé vers 1950 une notion d'équilibre très naturelle, qui généralisait celle donnée en 1838 par le mathématicien et économiste français Antoine Cournot. Étant données des actions que peuvent choisir des joueurs, ces actions forment un *équilibre de Nash* lorsque l'action de chaque joueur est la meilleure possible pour celui-ci, sachant que les autres joueurs choisissent éga-



Le mathématicien américain John Forbes Nash, né en 1928, a reçu le prix Nobel d'économie en 1994, notamment pour ses travaux en théorie des jeux. Vers l'âge de trente ans, Nash a commencé à souffrir de troubles mentaux graves, dont il s'est remis de manière spectaculaire au milieu des années 1980. Sa vie a d'ailleurs fait l'objet de la biographie « Un homme d'exception » et a inspiré le film du même titre. (Cliché Université de Princeton)

lement des actions spécifiées par l'équilibre de Nash. Dans une situation d'équilibre de Nash, personne n'a intérêt à changer unilatéralement son action.

La difficulté particulière des enchères, c'est que chaque joueur-enchérisseur est le seul à connaître sa propre évaluation du bien à vendre, et qu'il ne connaît pas les évaluations des autres acheteurs potentiels. Il faut donc généraliser le concept d'équilibre de Nash à cette situation, où l'information est incomplète. C'est ce qu'a réalisé intuitivement Vickrey en 1961 ; l'Américain d'origine hongroise John Harsanyi l'a fait plus rigoureusement vers 1967-1968, ce qui lui a valu aussi le prix Nobel, en 1994. On est ainsi parvenu à l'*équilibre de Nash bayésien*, notion d'équilibre qui permet d'émettre une conjecture sur la façon dont des enchérisseurs rationnels doivent miser dans une enchère.

Dans le contexte des enchères, une stratégie est, du point de vue mathématique, une fonction S qui associe à chaque évaluation d'un joueur sa mise correspondante. En d'autres termes, pour toute évaluation particulière v, cette fonction doit spécifier la mise $b^* = S(v)$ qui maximise l'espérance de gain calculée à partir des règles de l'enchère et en supposant que les autres joueurs utilisent la même stratégie. Cela signifie, dans un équilibre de Nash bayésien symétrique, que si les autres misent de la même façon, en employant la même stratégie, cette façon de miser est optimale. Pourquoi l'adjectif bayésien ? Parce que le joueur calcule une espérance de gain à partir des croyances qu'il a sur les évaluations des autres (en probabilités et statistiques, le point de vue bayésien — d'après Thomas Bayes, mathématicien anglais du XVIIIe siècle — consiste à évaluer des probabilités sur la base de l'information partielle disponible et de croyances *a priori*).

Quand la théorie confirme et étend l'intérêt de méthodes de vente conçues intuitivement…

Dans le domaine des enchères, les mathématiques ont donc permis de modéliser les comportements des acteurs, ce qui conduit à une prédiction sur leur façon de miser. Cela a permis de progresser dans deux directions. Sur le plan de la connaissance positive, il est devenu possible de confronter les données, c'est-à-dire les mises des joueurs dans différents types d'enchères, à ce que prédit la théorie. Celle-ci a, de ce fait, acquis un statut scientifique : on pourrait la rejeter au cas où l'on trouverait des données contredisant ses prédictions, la théorie est donc réfutable.

Sur le plan de l'établissement de normes, les conséquences ont été encore plus importantes. Dans le cadre des hypothèses de la théorie des enchères ainsi construite, on a pu démontrer un théorème assez fascinant : le *théorème de l'équivalence du revenu*. Sans entrer dans les détails, ce théorème prouve que les procédures d'enchères au premier ou deuxième prix (l'acheteur qui remporte le lot ne paye que le deuxième prix proposé) sous pli fermé, les enchères orales montantes (anglaises) ou descendantes (hollandaises) sont équivalentes pour le vendeur et qu'elles sont, de plus, souvent optimales. Ainsi, des méthodes de vente que l'on utilisait pragmatiquement dans des cas particuliers s'avéraient être, à la lumière de la théorie, la façon optimale d'allouer des ressources rares. D'où un enthousiasme nouveau pour l'extension de ces méthodes à toutes sortes d'activités éco-

nomiques. Enfin, dans des circonstances plus complexes que la vente d'un simple objet, la théorie permet de concevoir des généralisations des simples enchères pour optimiser davantage encore soit le revenu du vendeur, soit le bien-être social si l'organisateur des enchères est un État soucieux de cet aspect des choses. On a ainsi pu, grâce aux mathématiques, comprendre le sens et l'intérêt d'une pratique ancestrale et, par suite, transformer cette intuition humaine en un vrai outil de développement économique.

Avec Internet et les nouvelles technologies de communication, les enchères trouvent un champ immense d'expérimentations. Le réseau Internet offre à ce système de vente de nouvelles possibilités, que la théorie aidera à évaluer et à exploiter. Par exemple, dans une vente aux enchères, un vendeur anonyme devrait *a priori* souffrir de l'asymétrie d'information — lui seul connaît la qualité des biens qu'il vend — et ne réussir qu'à obtenir un prix de vente très faible ; mais par des ventes répétées d'objets de qualité *a priori* inconnue des acheteurs potentiels, il va pouvoir petit à petit se construire une réputation, grâce aux commentaires qu'apporteront ses anciens acheteurs. La qualité des échanges pourra donc être améliorée en créant un lieu où peuvent se bâtir des réputations de qualité et d'honnêteté, ce à quoi se prête aisément un site Internet.

Jean-Jacques Laffont
Institut d'économie industrielle,
Université des sciences sociales,
Manufacture des tabacs, Toulouse

Quelques références :

- I. Ekeland, *La théorie des jeux et ses applications à l'économie mathématique* (P.U.F., 1974)
- A. Cournot (1838), *Recherche sur les principes mathématiques de la théorie des richesses* (Calmann-Lévy, Paris, rééd. 1974).
- J. Crémer et J.-J. Laffont, « Téléphonie mobile », *Commentaire, 93*, 81-92 (2001).
- L. Friedman, « A Competitive bidding strategy », *Operations Research, 4,* 104-112 (1956).
- J. Harsanyi, « Games with incomplete information played by bayesian players », *Management Science, 14*, 159-182, 320-134, 486-502 (1967-1968).
- J.-J. Laffont, « Game theory and empirical economics : the case of auction data », *European Economic Review, 41*, 1-35 (1997).

De l'économétrie pour vendre des vins ou des obligations

Philippe Février et Michael Visser

Grands vins ou bons du Trésor font l'objet de ventes aux enchères. Mais quel type d'enchères faut-il pratiquer ? Pour le savoir, on complète les modélisations générales des enchères par des études économétriques.



Une vente aux enchères (à la bougie) de vins aux hospices de Beaune, en Bourgogne. Des analyses économétriques indiquent que le recours aux options d'achat permet d'augmenter le revenu du commissaire-priseur. (Cliché Gamma/Alexis Orand)

Dans les salles de vente de Richelieu-Drouot, les ventes aux enchères de vins sont des enchères ascendantes classiques, ou *enchères anglaises*. Dans une telle procédure, le commissaire-priseur annonce un prix de départ peu élevé, puis augmente progressivement ce prix jusqu'à ce qu'il ne reste qu'un seul enchérisseur, les autres ayant abandonné. L'objet à vendre est acquis par ce dernier au prix atteint. Lorsque plusieurs lots de vin identiques doivent être mis aux enchères, un mécanisme appelé option d'achat permet au gagnant d'un lot dans une enchère de choisir le nombre de lots qu'il souhaite acquérir au même prix (si l'*option d'achat* n'est pas disponible, les lots sont mis successivement aux enchères). Considérons par exemple le cas de la vente de deux lots identiques de six bouteilles Mouton-Rotschild 1945. La première enchère terminée, le commissaire-priseur propose au gagnant d'obtenir le deuxième lot au même prix que le premier. Si le gagnant exerce son option, il n'y a pas de deuxième enchère et les deux lots sont attribués au gagnant de la première enchère. Si le

gagnant n'exerce pas son droit, le deuxième lot est alors mis aux enchères.

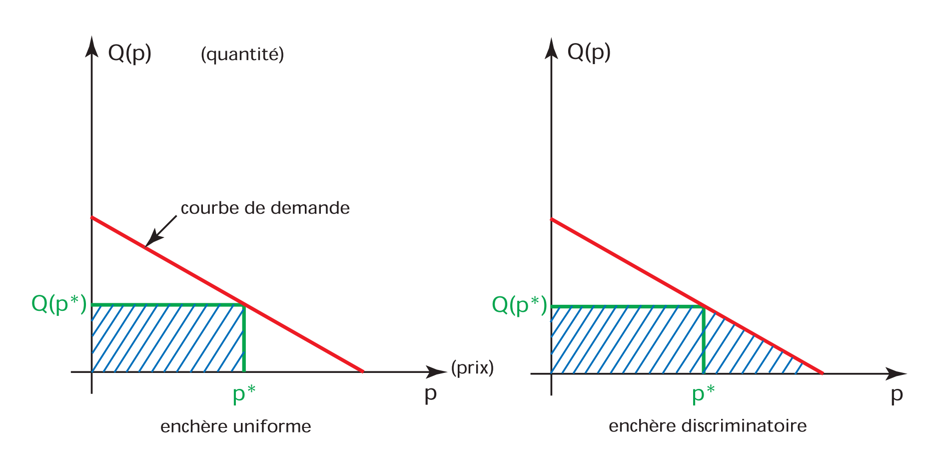
L'option d'achat permet bien sûr d'accélérer les ventes, mais elle induit aussi une composante stratégique. Il est clair en effet que les enchérisseurs ne se comportent pas de la même façon avec ou sans option d'achat. Dans le premier cas, la perte du premier lot implique potentiellement la perte des deux lots si le gagnant utilise son option, ce qui n'est pas le cas en l'absence d'option. Quel est donc l'impact stratégique de l'option d'achat ? La présence de l'option d'achat incite-t-elle les enchérisseurs à enchérir davantage que dans le cas contraire et donc augmente-t-elle le revenu du vendeur ?

L'État doit-il pratiquer des enchères uniformes ou discriminatoires ?

L'État français finance sa dette en émettant des obligations appelées bons du Trésor. L'attribution de ces obligations se fait à l'aide d'une procédure d'enchère dite *discriminatoire*. Chacun des enchérisseurs, appelés spécialistes en valeur du Trésor ou SVT, établit un ensemble de couples prix-quantité *(p, Q (p))* qui définit, selon le prix *p* d'un bon du Trésor, la quantité *Q (p)* de bons qu'il souhaite acheter. L'État ayant au préalable annoncé la quantité totale *T* d'obligations qu'il désirait émettre, la demande agrégée (la somme des demandes individuelles des enchérisseurs) détermine un prix dit d'équilibre p^* : c'est le prix p^* tel que $T = Q_1 (p^*) + Q_2 (p^*) + \ldots + Q_N (p^*)$, où Q_i est la quantité de bons souhaitée par le *i*-ème SVT. Chacun de ces derniers obtient alors la quantité $Q_i (p^*)$ de bons qu'il a demandée.

Si le prix que chaque enchérisseur payait pour une obligation était p^*, il s'agirait d'une enchère dite *uniforme*, et le coût total pour l'enchérisseur serait alors simplement $p^*Q (p^*)$, le prix d'un bon multiplié par le nombre de bons demandés (c'est l'aire du rectangle hachuré dans le graphique de gauche). Mais dans l'enchère dite *discriminatoire* à laquelle l'État recourt, le prix payé n'est pas p^* pour chaque obligation, mais un peu supérieur. En effet, l'État fait payer aux enchérisseurs le maximum de ce qu'ils étaient prêts à payer pour chaque obligation supplémentaire ; le coût total pour l'enchérisseur est représenté par l'aire hachurée dans le graphique de droite.

Illustrons-le par l'exemple d'un enchérisseur dont la courbe de demande est la sui-



*Dans une enchère uniforme sur les bons du Trésor, l'enchérisseur paie la somme p*Q (p*) (aire de la surface hachurée dans le graphique de gauche), où p* est le prix dit d'équilibre d'un bon, déterminé en fonction de la demande de tous les enchérisseurs, et Q (p*) la quantité de bons demandée au préalable par l'enchérisseur pour ce prix. Dans une enchère discriminatoire, l'enchérisseur paie un prix plus élevé que p*Q (p*), correspondant à l'aire hachurée dans le graphique de droite. Les stratégies des enchérisseurs ne sont pas les mêmes dans ces deux types d'enchère.*

vante : il demande 10 obligations si le prix est de 90 euros, 9 obligations si le prix est de 100 euros, ..., 1 obligation si le prix est de 180 euros. En supposant que le prix d'équilibre p^* est de 130 euros, cet enchérisseur recevra 6 obligations. Dans une enchère discriminatoire, le prix qu'il payera est le prix maximal qu'il était prêt à payer pour ces 6 obligations, à savoir : 180 euros pour la première, 170 euros pour la deuxième, ..., 130 euros pour la sixième, soit un total de 930 euros. Dans la procédure d'enchère uniforme, cet enchérisseur aurait payé 130 euros chacune des six obligations, soit un total de 780 euros.

Évidemment, les SVT n'enchérissent pas de la même manière dans les deux types d'enchère et la comparaison des deux mécanismes n'a rien d'immédiat. Le Mexique a changé de procédure d'enchère en 1990 pour privilégier l'enchère discriminatoire. Les États-Unis, au contraire, ont abandonné en 1998 l'enchère discriminatoire pour l'enchère uniforme. L'enchère uniforme est-elle plus rentable pour l'État ? La France devrait-elle aussi changer de mode d'adjudication ?

On doit comparer deux situations alors qu'il n'existe de données que sur une seule d'entre elles

Les réponses à ces questions, concernant l'option d'achat pour les vins ou les enchères discriminatoires pour les obligations, sont importantes. Les montants en jeu peuvent être considérables : 185 milliards d'euros en l'an 2000 pour les adjudications des bons du Trésor, plusieurs dizaines de millions d'euros par an pour Drouot. Comment résoudre des problèmes de ce type ? La méthode la plus efficace consisterait à organiser une expérience réelle. Ainsi, dans les enchères de bons du Trésor, il faudrait recourir aux deux modes d'enchères en parallèle pour comparer les résultats. De même, pour les ventes de vins aux enchères, il faudrait pratiquer les deux modes d'enchère, avec et sans option d'achat, pour comparer le comportement des enchérisseurs. Malheureusement, il est très rarement possible de mettre en place de telles expériences. Nous sommes donc confrontés au problème suivant : comparer deux situations en n'ayant des informations *a priori* que sur une seule d'entre elles.

La solution de notre problème fait intervenir une démarche mathématique complexe. Dans un premier temps, il faut modéliser les comportements des enchérisseurs. Les enchérisseurs sont caractérisés par le prix maximum qu'ils sont prêts à payer pour obtenir l'objet en vente, prix que l'on appelle leur évaluation. Dans ce modèle, chaque joueur connaît sa propre évaluation, mais ignore celles des autres joueurs. Il n'a en fait qu'un *a priori* sur les possibles valeurs que peuvent prendre ces évaluations et cet *a priori* peut être représenté par une fonction f qui spécifie avec quelle probabilité ces différentes valeurs sont prises : $f(v)$ est la probabilité que l'enchérisseur attribue la valeur v au bien à vendre. La stratégie d'enchère optimale, c'est-à-dire le prix que doit offrir l'enchérisseur en fonction de son évaluation, est obtenue par la recherche de l'équilibre de Nash bayésien (voir l'article précédent, de Jean-Jacques Laffont).

On peut ainsi modéliser d'un point de vue théorique les deux situations concrètes que l'on veut analyser, ce qui permet de les comparer théoriquement. Cette comparaison dépend évidemment de la fonction f choisie. Si, quelle que soit la fonction f, l'une des deux

situations domine l'autre (par exemple l'enchère discriminatoire permet à l'État d'obtenir un revenu plus important que l'enchère uniforme quelles que soient les croyances des SVT, définies par la fonction *f*), il est possible de conclure. En général, les situations analysées sont trop complexes pour qu'une telle dominance apparaisse. Nous obtenons alors à ce stade des conclusions du type : si la fonction *f* est celle-ci, alors Drouot a intérêt à maintenir l'option d'achat, mais si la fonction *f* est celle-là, ce n'est plus le cas. Le problème revient donc à celui de la connaissance effective de cette fonction *f*.

C'est la confrontation entre les données réelles et les prévisions de la théorie qui permet de déterminer *f*. En effet, si l'on choisit une fonction donnée *f*, le modèle et les stratégies d'équilibre calculées dans le modèle de comportement nous disent ce que les joueurs auraient dû enchérir. Il suffit alors de comparer ces prédictions — calculables puisque nous avons fait un choix pour *f* — avec les données réelles. Si elles coïncident, c'est que la fonction choisie pour *f* était la bonne ; sinon, il faut recommencer avec une autre fonction.

Deux types de méthodes économétriques pour déterminer les probabilités attachées aux évaluations des enchérisseurs

En pratique, il n'est pas possible d'essayer l'une après l'autre toutes les fonctions *f* imaginables : il y en a une infinité ! Pour déterminer *f*, on doit faire appel à des méthodes dites *économétriques*. On peut les classer en deux grandes catégories : les méthodes paramétriques (dans lesquelles on suppose que la fonction *f* est complètement caractérisée par un certain nombre de paramètres inconnus) et les méthodes non paramétriques (qui ne font aucune hypothèse *a priori* sur *f*). Ces dernières, plus générales mais aussi plus compliquées, ont été développées à partir de la fin des années 1950, mais ce n'est que très récemment que les chercheurs ont réussi à les adapter au problème de l'estimation de notre fameuse fonction *f*. Une fois trouvée cette fonction *f* (ou, de manière équivalente, les valeurs des paramètres définissant *f* dans les méthodes paramétriques), il suffit de comparer les deux situations étudiées pour savoir laquelle domine l'autre, laquelle est la plus avantageuse du point de vue du vendeur.

Option d'achat, enchère discrimatoire : les modèles montrent que ces procédures sont avantageuses pour le vendeur

C'est cette démarche qui nous a permis de répondre aux questions posées au début de cet article sur l'utilisation de l'option d'achat dans les enchères de vin à Drouot. Nous avons dans un premier temps développé deux modèles théoriques, l'un avec option d'achat et l'autre sans, et calculé les équilibres bayésiens dans les deux situations. Nous nous sommes alors rendus à Drouot pour obtenir des données (prix de vente des vins, caractéristiques de ces vins, etc.), puis nous avons appliqué une méthode d'estimation paramétrique à notre modèle théorique avec option d'achat. Il est important de noter que tous les vins ne sont pas identiques (année, couleur, château, niveau, étiquette, etc.) et qu'il faut procéder à une estimation de la fonction *f* pour chaque catégorie de vin. Une fois ces estimations réalisées, le modèle théorique sans option d'achat nous a permis de calculer le

revenu qu'aurait eu le commissaire-priseur s'il n'avait pas utilisé l'option d'achat. Les premières conclusions de cette étude sont que l'utilisation de l'option d'achat permettrait aux commissaires-priseurs d'augmenter leur revenu de 7 % par rapport à la situation sans option d'achat.

À partir de données sur les ventes françaises de bons du Trésor en 1995, nous avons mis en œuvre le même type de démarche pour comparer les deux modes d'adjudication (enchère uniforme *versus* enchère discriminatoire). Les résultats de ces travaux montrent qu'avec l'enchère discriminatoire, le revenu de l'État est supérieur de 5 % à celui obtenu avec une enchère uniforme. Ainsi, dans ce problème comme dans celui des enchères de vins, des modèles économétriques élaborés apportent des réponses à des questions auxquelles il pouvait sembler impossible de répondre, de par l'absence de données concernant l'une des deux situations à comparer.

Philippe Février [1, 2] et Michael Visser [1]
[1]CREST-LEI (Centre de recherche en économie et statistique-Laboratoire d'économie industrielle, Paris)
[2]INSEE (Institut national de la statistique et des études économiques)

Quelques références :

- C. Gouriéroux et A. Monfort, *Statistique et modèles économétriques* (Economica, 1989).
- P. Février, W. Roos et M. Visser, « Etude théorique et empirique de l'option d'achat dans les enchères anglaises », Document de travail du CREST (2001).
- J.-J. Laffont, H. Ossard et Q. Vuong, « Econometrics of first price auctions », *Econometrica, 63*, pp. 953-980 (1995).
- S. Donald et H. Paarsch, « Piecewise pseudo-maximum likelihood estimation in empirical models of auctions », *International Economic Review, 34*, pp. 121-148 (1993).
- P. Février, R. Préget et M. Visser, « Econometrics of Share Auctions », Document de travail du CREST (2001).
- E. Guerre, I. Perrigne et Q. Vuong, « Optimal nonparametric estimation of first price auctions », *Econometrica, 68*, pp. 525-574 (2000).
- W. Härdle, *Applied nonparametric regression* (Cambridge University Press, 1990).

Les casse-tête des compagnies aériennes



Jean-Christophe Culioli

Les problèmes d'organisation et de planification posés à une compagnie aérienne sont analogues à ceux rencontrés dans d'autres secteurs d'activité. La recherche opérationnelle, domaine qui concerne des dizaines de milliers de mathématiciens et d'ingénieurs dans le monde, s'évertue à les résoudre au mieux.

Le transport aérien est une activité complexe. Celle-ci met en jeu des investissements lourds (les avions et les infrastructures de maintenance), du personnel hautement qualifié (comme le personnel navigant) et une informatique à temps réel coûteuse (les systèmes de réservation et de gestion). C'est aussi un secteur où la concurrence est exacerbée, où les prix affichés ne reflètent pas toujours les coûts de production instantanés. Pour qu'elle soit à la fois compétitive et sûre, une compagnie aérienne doit donc être gérée au plus juste.

Pour ce faire, elle doit faire appel à des techniques d'optimisation spécifiques à chacune des étapes de la production. On regroupe ces techniques mathématiques sous le nom de *recherche opérationnelle*. Ce domaine est né sous l'impulsion des besoins militaires anglo-saxons durant la Deuxième guerre mondiale, avec les débuts des ordinateurs et des méthodes dites de programmation linéaire (voir l'encadré). La recherche opérationnelle s'est, depuis, beaucoup développée et a largement pénétré le monde des entreprises et de l'industrie. Étant donnés les enjeux, ses méthodes sont parfois confidentielles.



Pour utiliser au mieux sa flotte, une compagnie aérienne doit établir soigneusement ses programmes de maintenance et ses programmes de vols, planifier le travail des personnels au sol et les rotations d'équipages, etc. Ce sont des problèmes difficiles de recherche opérationnelle, qui font intervenir des équations à plusieurs milliers d'inconnues. (Cliché Air France)



La recherche opérationnelle est censée résoudre des questions d'emploi du temps, d'affectation de tâches, d'ordonnancement d'étapes de fabrication, etc., où interviennent de multiples variables et contraintes, la solution devant être la meilleure possible — au sens d'un meilleur coût, d'un délai minimal, ou autre. Un exemple élémentaire de problème de recherche opérationnelle est celui d'affecter, dans une entreprise qui comporte 50 postes de travail, un poste déterminé à chacun des 50 employés, en tenant compte au mieux des aptitudes de chacun. Pour obtenir la meilleure solution à ce problème, on pourrait bien sûr passer en revue toutes les possibilités, évaluer chacune puis choisir la plus avantageuse. C'est tout à fait exclu en pratique : il faudrait explorer $50! = 50 \times 49 \times 48 \times ... \times 3 \times 2 \times 1$ possibilités, un nombre faramineux (égal à environ 3×10^{64}). Même si un ordinateur pouvait parcourir un milliard de possibilités par seconde, il lui faudrait 10^{48} années pour les épuiser toutes, beaucoup plus que l'âge estimé de l'Univers (environ 10^{10} ans) !

Cet exemple laisse entrevoir l'ingéniosité que doit déployer la recherche opérationnelle pour traiter de tels problèmes de façon réaliste, en un temps de calcul acceptable. En plus des outils informatiques, des techniques mathématiques diverses et variées (algébriques, probabilistes, numériques, etc.) entrent dans la conception de ses méthodes. Bien que née il y a plus de cinquante ans, la recherche opérationnelle est une science mathématique toujours jeune : il ne se passe guère plus de trois ans entre le moment où une méthode est conçue dans un laboratoire de recherche et le moment où elle passe en production, après avoir passé l'étape du bureau d'études. Dans le secteur aérien, les enjeux sont tels qu'ils ont suscité la création de nombreuses sociétés de conseils et services mathématiques et informatiques comme le groupe *Sabre*, issu du département de recherche opérationnelle de la compagnie American Airlines, la société *Adopt* issue du laboratoire *Gerad* (Groupe d'études et de

La programmation linéaire

La programmation linéaire est le problème mathématique consistant à déterminer des quantités positives $x_1, x_2, \dots, x_N$ qui minimisent un certain « coût », supposé égal à $c_1x_1 + c_2x_2 + \dots + c_Nx_N$, où les $c_1, c_2, \dots, c_N$ sont des nombres connus, et les x_i étant par ailleurs soumis à des contraintes s'exprimant par des équations linéaires (de la forme $A_1x_1 + A_2x_2 + \dots + A_Nx_N = B$, où les A_i et B sont des nombres connus, qui dépendent du problème posé). De très nombreuses questions de recherche opérationnelle peuvent se formuler en ces termes. Si l'énoncé du problème de programmation linéaire est relativement simple, sa résolution ne l'est pas du tout, d'autant que le nombre N d'inconnues à déterminer atteint, dans la pratique, plusieurs milliers. Ce problème d'apparence anodine, mais de première importance pour les applications, est à l'origine des recherches les plus fructueuses en optimisation depuis une trentaine d'années. En 1947, le mathématicien américain George Dantzig proposait l'excellent et encore fréquemment utilisé algorithme du simplexe. Dans les années 1970 et 1980, d'autres algorithmes concurrents sont apparus. L'année 1984 a marqué un tournant : un jeune mathématicien travaillant aux États-Unis, Narendra Karmarkar, découvrait un algorithme de programmation linéaire particulièrement efficace (convergence dite polynomiale). Les idées sous-jacentes à sa méthode ont inauguré un courant de recherche très actif (méthodes de points intérieurs), qui a mobilisé simultanément des milliers de mathématiciens dans le monde. Grâce à ces efforts, l'industrie dispose à présent d'une palette d'algorithmes de programmation linéaire très performants.

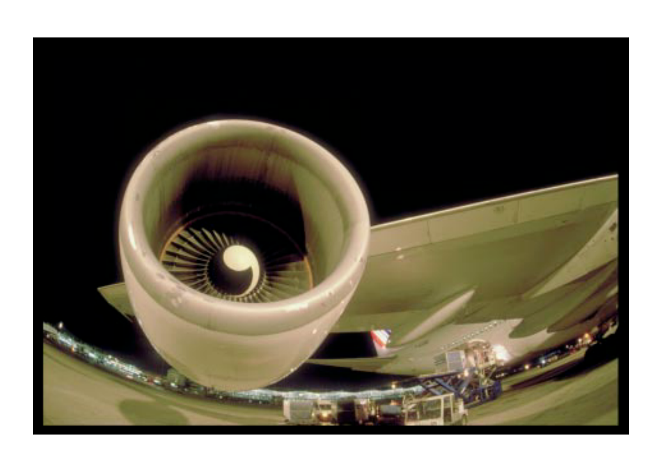


recherche en analyse des décisions) de l'université de Montréal, ou des sociétés françaises comme *Eurodecision*, *Ilog*, ou *Cosytech*.

Optimiser le programme de vols, attribuer un appareil à chaque vol, minimiser les temps d'immobilisation

Pour utiliser au mieux la flotte d'appareils, première richesse d'une compagnie aérienne, il faut commencer par établir un programme de maintenance optimal, en positionnant dans le temps les petites et grandes visites techniques que doit subir chaque avion. Un avion au sol ne rapportant aucune recette, on doit minimiser le temps d'immobilisation de chaque appareil en tenant compte des horaires et des qualifications des agents, de la disponibilité des hangars, etc. Les équations qui traduisent le problème ne sont pas linéaires. Elles présentent donc quelques difficultés, mais on dispose depuis peu de méthodes suffisamment efficaces pour les traiter.

Une fois le programme de maintenance établi (sur un horizon de 6 mois à 10 ans) il s'agit d'établir un programme de vol optimisé.



Les compagnies aériennes cherchent à réduire le plus possible les temps d'immobilisation au sol de leurs appareils, en tenant compte de contraintes multiples : au sol, un avion ne rapporte aucune recette. (Cliché Air France)

Après avoir construit un réseau — une liste de parcours à réaliser avec des horaires associés, en fonction de prévisions de parts de marchés et de fenêtres attribuées à chaque compagnie par l'IATA (International Airline Transportation Association) — on détermine quel type d'avion (Airbus 340, par exemple) sera le plus adapté, techniquement et économiquement, pour effectuer chacun de ces vols. Les données qui entrent dans les programmes d'optimisation sont les caractéristiques des avions (capacité, performances), les flux prévisionnels de passagers, etc. L'élaboration du programme de vols nécessite des techniques d'optimisation faisant appel aux statistiques et aux probabilités, ainsi qu'à des algorithmes de programmation linéaire dite en nombre entiers (où les inconnues représentent des nombres entiers).

Il s'agit ensuite d'enchaîner les vols et les opérations de maintenance de chacun des avions de manière à satisfaire l'ensemble des contraintes opérationnelles (successions autorisées ou non, règles de maintenance, etc.), tout en minimisant les conséquences éventuelles de pannes techniques, de retards imprévus, etc. Ce problème d'optimisation, connu sous le nom de construction de rotations d'avions, est modélisé comme un programme linéaire en nombres entiers de très grande taille. Il nécessite, pour être résolu exactement, l'application d'une technique de décomposition (*la génération de colonnes, relaxation lagrangienne*).

Enfin, pour chaque rotation d'avion, il faut déterminer quel avion exactement lui sera affecté en fonction des contraintes de maintenance de chaque appareil (nombre d'heures de vol, nombre de cycles d'atterrissages/décollages avant visite, etc.). Cette *matriculation* est généralement réalisée par une recherche



de type « programmation dynamique ». Introduite par l'Américain Richard Bellman dans les années 1950, cette démarche consiste à décomposer le problème de décision initial en plusieurs problèmes plus simples qui peuvent être résolus l'un à la suite de l'autre (la programmation dynamique peut s'appliquer aussi bien au calcul des trajectoires optimales d'avions qu'à la détermination de stratégies financières d'investissement).

Les problèmes de planification revêtent des formes diverses ; les mathématiques sous-jacentes aussi

Chaque avion ayant un programme bien précis prévu à l'avance, on peut alors tenter de maximiser sa recette attendue en ouvrant ou fermant les classes de réservation selon la demande effective de la clientèle. Ce problème est très classique dans l'aviation, le transport ferroviaire de passagers, chez les loueurs de voitures et les chaînes hôtelières. Il se pose comme un problème d'optimisation stochastique, où il faut maximiser une recette F au sens des probabilités, c'est-à-dire maximiser l'espérance mathématique de la recette F sachant que F dépend de variables aléatoires x_i (les x_i peuvent par exemple représenter les effectifs de chaque classe de réservation, avec des contraintes de la forme $A_1x_1 + A_2x_2 + \ldots + A_Nx_N = B$, où B représente une capacité).

À tout ce qui précède, il faut ajouter la planification des personnels au sol (taille des effectifs, synchronisation avec les programmes de vol, programmation de la prise en charge des passagers en correspondance et de leurs bagages, etc.) et celle du personnel navigant, en tenant compte bien sûr de la réglementation du travail et des normes de sécurité. On le voit, l'activité d'une compagnie aérienne pose une grande variété de problèmes d'optimisation, qui sont d'ailleurs souvent analogues à ceux du transport ferroviaire ou maritime. Ces problèmes sont difficiles ; mathématiquement, ils correspondent à la minimisation ou la maximisation de quantités dépendant d'un grand nombre de variables (souvent plusieurs milliers, voire plus). Néanmoins, les efforts de la recherche opérationnelle ont porté leurs fruits, et l'on dispose aujourd'hui de très bons algorithmes pour la plupart des situations. Mais personne dans ce domaine ne s'endort sur ses lauriers : comme les performances de l'entreprise en dépendent, les recherches doivent se poursuivre.

Jean-Christophe Culioli
Directeur de la recherche opérationnelle
Air France

Quelques références :

- Y. Nobert, R. Ouellet et R. Parent, *La recherche opérationnelle* (3e éd., Gaëtan Morin, 2001).
- R. Faure, B. Lemaire et C. Picouleau, *Précis de recherche opérationnelle* (5e éd., Dunod, 2000).
- « AirWorthy OR » dans *Operational Research and Management Science Today*, numéro de décembre 1999.
- Bulletins de la ROADEF (Association pour la Recherche Opérationnelle et l'Aide à la Décision en France, issue de la refondation de l'AFCET).

De la géométrie à 11 dimensions pour comprendre la Genèse ?

Maurice Mashaal

Les physiciens aspirent depuis longtemps à une théorie capable d'englober toutes les particules élémentaires et toutes leurs interactions. Depuis une quinzaine d'années, ils ont une piste sérieuse. Mais pour l'explorer, ils doivent naviguer dans des espaces hautement abstraits où même les mathématiciens ne s'étaient pas encore aventurés.

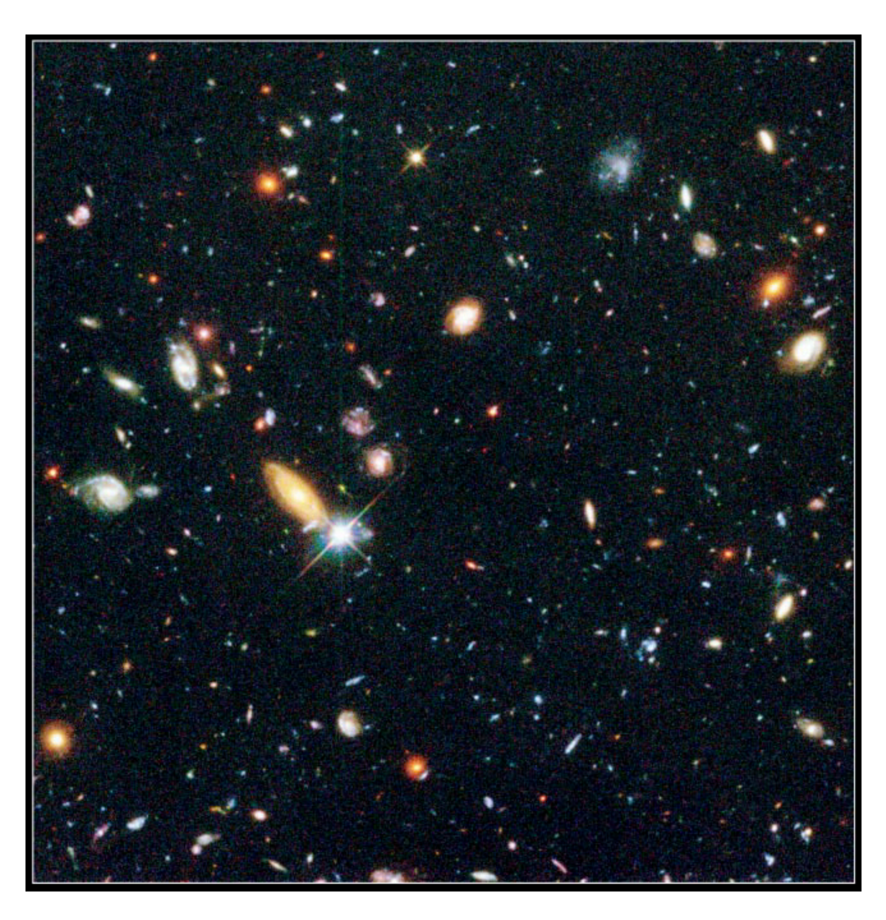
Tout honnête homme sait que les scientifiques comme les physiciens ou les chimistes utilisent des mathématiques. Plus rares sont ceux qui savent à quel point cela est vrai, et combien profonde est l'imbrication entre mathématiques et sciences de la nature. Galilée a dit que le livre de la Nature est écrit en langage mathématique. Cette idée, le développement de la science moderne, et plus particulièrement celui de la physique, semble la confirmer pleinement. Il y a même plus qu'une confirmation : bien des penseurs s'étonnent de constater que les inventions ou découvertes mathématiques ont toujours fini par servir à la description de quelque aspect des phénomènes naturels. C'est l'étonnement devant la fameuse « déraisonnable efficacité des mathématiques dans les sciences de la nature » dont parlait le physicien d'origine hongroise Eugene P. Wigner (1902-1995).

On ne sait pas vraiment pourquoi les mathématiques sont si « efficaces ». C'est une question encore ouverte, qui concerne la philosophie de la connaissance. On n'essaiera pas ici d'y répondre, mais seulement d'illustrer cette efficacité dans le domaine de la physique la plus théorique et la plus fondamentale, celle qui n'a *a priori* aucune utilité matérielle — et de laquelle pourtant ont résulté des inventions cruciales comme le laser, le transistor ou l'énergie nucléaire…

Physique et mathématiques, une longue histoire d'apports réciproques

Les liens entre mathématiques et physique ne datent pas d'aujourd'hui. Le principe d'Archimède (« tout corps plongé dans un liquide subit une poussée égale au poids du volume de liquide déplacé ») ne constitue-t-il pas un énoncé mathématique portant sur un phénomène physique ? La physique n'a-t-elle pas connu des progrès spectaculaires grâce à la création du calcul différentiel et intégral par Newton et Leibniz, au XVIIe siècle ? Qui plus est, ces liens ne sont pas toujours à sens unique,

un outil mathématique étant d'abord inventé puis appliqué à un problème de physique. Un exemple parmi bien d'autres en témoigne : c'est en s'intéressant au problème de la propagation de la chaleur que le mathématicien français Jean-Baptiste Joseph Fourier (1768-1830) a conçu les « séries de Fourier » (il s'agit de sommes infinies de fonctions trigonométriques), qui jouent depuis un rôle extrêmement important dans les sciences et les techniques.



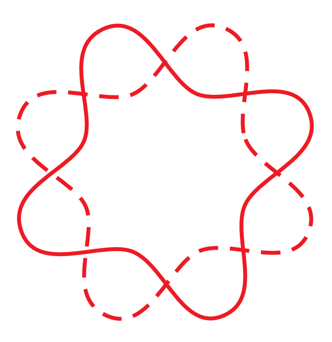
Une myriade de galaxies très lointaines vues par le télescope spatial Hubble. La gravitation étant un élément clef de la naissance et de l'évolution de l'Univers, les spécialistes de cosmologie aimeraient disposer enfin d'une description de la force de gravitation compatible avec les principes de la physique quantique. La théorie des cordes exaucera-t-elle ce vœu ? (Cliché R. Williams/HDF (STSci)/NASA)

La physique du XXe siècle est riche en interactions avec les mathématiques. C'est le cas avec les deux grandes théories nées aux début de ce siècle, la théorie de la relativité d'Einstein et la mécanique quantique. La relativité (générale) d'Einstein est une théorie de la gravitation qui supplante celle de Newton ; elle repose sur des concepts radicalement différents, liés aux géométries non euclidiennes, introduites au XIXe siècle, quand personne ne soupçonnait que de telles mathématiques puissent avoir un quelconque rapport avec la réalité. De même, quand des mathématiciens ont commencé à étudier les « espaces de Hilbert » (espaces abstraits dont les points peuvent être — par exemple — des fonctions vérifiant certaines conditions techniques), au début des années 1900, personne ne se doutait qu'une vingtaine d'années plus tard, les mathématiques des espaces de Hilbert allaient constituer le cadre adéquat pour formuler les lois de la mécanique quantique (qui se manifestent surtout à l'échelle atomique et subatomique). Réciproquement, les recherches fondamentales en relativité générale ou en mécanique quantique ont à leur tour stimulé des recherches purement mathématiques.

La physique des particules élémentaires, champ où se déploient des mathématiques très abstraites

Regardons d'un peu plus près l'une des voies dans laquelle s'est développée la physique quantique : l'étude des particules dites

élémentaires et de leurs interactions. Au cours des décennies 1930-1950, s'est élaboré un cadre théorique d'une grande complexité, tant du point de vue des concepts que des techniques mathématiques mises en œuvre, appelé la *théorie quantique des champs*. C'est dans ce cadre, et avec la mise en évidence de nouvelles particules grâce aux accélérateurs de particules, que les physiciens ont découvert que le monde des particules élémentaires manifeste un certain nombre de symétries. La *théorie des groupes*, une importante branche des mathématiques fondée au XIXe siècle, a joué et continue à jouer un rôle capital dans l'élucidation de ces symétries (abstraites pour la plupart). C'est grâce à



Une corde fermée vibre de façon à présenter un nombre entier de crêtes et de creux. Les différentes particules subatomiques (électrons, photons, etc.) correspondraient aux différents modes de vibration de minuscules cordes fondamentales.

elle que, à plusieurs reprises, les théoriciens ont pu prédire l'existence de certaines particules, quelques années avant qu'elles ne soient découvertes par les expérimentateurs.

Dans les années 1970-1980, la théorie des particules élémentaires était parvenue au point où elle était capable de décrire de manière satisfaisante et unifiée toutes les particules connues et presque toutes leurs interactions. Pourquoi « presque » ? On connaît quatre interactions fondamentales — la force gravitationnelle, la force électromagnétique et deux forces agissant à l'échelle nucléaire, l'interaction faible et l'interaction forte ; or les physiciens n'ont pas réussi à faire entrer la force gravitationnelle dans leur théorie, appelée le *Modèle standard* de la physique des particules.

Concilier la gravitation avec la physique quantique : un défi fondamental qui semble à la portée de la théorie des cordes

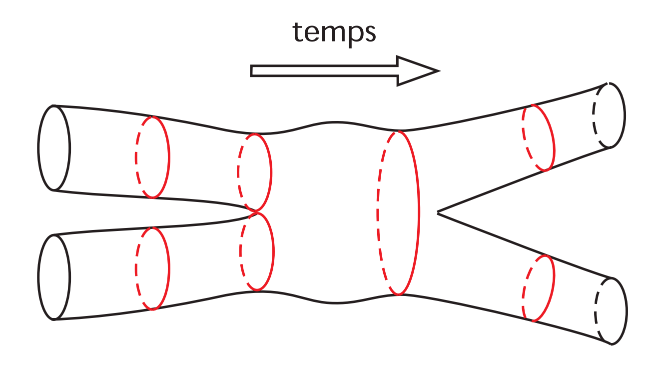
Que signifie cette exception ? La gravitation semble correctement décrite par la relativité générale d'Einstein, mais la théorie d'Einstein n'est pas une théorie quantique, c'est-à-dire qu'elle n'intègre pas les principes (assez étranges, soit dit en passant) de la physique quantique. Or on ne voit pas du tout pourquoi, alors que toute la nature obéit aux lois quantiques, la gravitation en serait dispensée. D'où l'obstination des physiciens théoriciens de faire rentrer la gravitation dans le bercail quantique. Malgré plusieurs décennies d'efforts, ils n'y sont pas arrivés.

Cependant, depuis le milieu des années 1980, beaucoup d'entre eux croient que l'on tient le bon bout. En effet, c'est à cette époque qu'une nouvelle théorie encore inachevée mais prometteuse, appelée *théorie des cordes*, a gagné suffisamment de cohérence pour qu'on l'envisage sérieusement. Le contexte exact et les raisons précises qui ont poussé les théoriciens dans cette direction sont beaucoup trop techniques pour qu'on les explique ici. Il est également impossible d'expliquer de façon simple en quoi consiste la théorie des cordes. Disons juste, de façon très approximative, qu'elle suppose que les objets physiques fondamentaux ne sont pas des particules assimilées à des points (« philosophie » des théories

quantiques de champs traditionnelles), mais de minuscules cordes sans épaisseur — de petits morceaux de ligne, en quelque sorte ; et que les différentes particules observées à notre échelle correspondraient aux différents modes de vibration des cordes, un peu comme les différents modes de vibration d'une corde de violon correspondent aux différentes notes musicales.

Pour que les théories des cordes soient cohérentes, il faut que l'espace-temps possède 11 dimensions

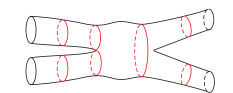
Les théories des cordes (*théories* au pluriel, car il en existe en fait plusieurs variantes) sont encore préliminaires et d'une complexité redoutable. Nombre de leurs aspects restent à défricher. De plus, il est pour le moment impossible de les mettre à l'épreuve de l'expérience, car les énergies que cela demanderait sont tout à fait inaccessibles, même avec les accélérateurs de particules les plus puissants dont nous disposons. Mais elles ont séduit les théoriciens, parce que ces théories (quantiques) intègrent de façon naturelle la gravitation, apparemment sans se heurter aux obstacles qui surgissaient dans les théories précédentes.

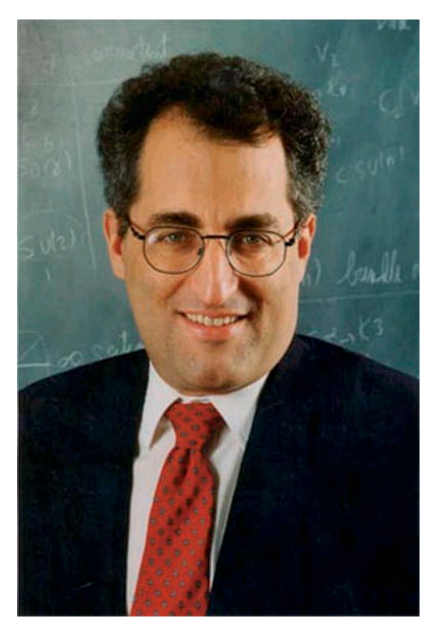


Représentation schématique de l'interaction entre deux cordes. Au cours du temps, qui s'écoule de gauche à droite dans ce schéma, une corde fermée balaie une surface analogue à un tube.

Si les physiciens réussissent à construire une théorie des cordes complète et cohérente, ils seront en mesure d'étudier de façon précise les phénomènes gravitationnels violents (de très haute énergie) qui se déroulent dans le cosmos, comme l'effondrement d'une grosse étoile sur elle-même, la physique des « trous noirs », etc. Ce sont aussi les mystères des tout premiers instants de la naissance de l'Univers — les premiers instants du fameux big bang, événement violent s'il en est — que l'on pourra mieux cerner. Une description quantique de la gravitation permettra certainement de faire un saut qualitatif et quantitatif dans la compréhension de l'Univers, de son origine et de son évolution.

Mais comme on l'a dit plus haut, les théories des cordes sont très compliquées. Elles impliquent des techniques mathématiques élaborées, souvent issues des recherches les plus récentes. De fait, les spécialistes qui étudient ces théories comprennent indifféremment des physiciens et des mathématiciens (plusieurs lauréats de la médaille Fields, la récompense suprême en mathématiques, ont consacré une part importante de leurs travaux aux théories des cordes ; c'est le cas de l'Américain Edward Witten, ou du Russe installé en France Maxim Kontsevitch). Il a été notamment établi que les théories des cordes ne peuvent être cohérentes que si l'on suppose que l'espace-temps possède non pas quatre dimensions (trois dimensions pour l'espace, une dimension pour le temps), mais bien davantage : 11 dimensions aux dernières nouvelles ! Les sept dimensions supplémentaires, imperceptibles à nos sens car elles seraient refermées sur elles-mêmes en de minuscules





Edward Witten, l'un des principaux artisans de la théorie des cordes. On ne sait s'il faut le considérer comme un physicien ou comme un mathématicien… (Cliché : DR)

boucles, contribuent à l'abstraction et à la difficulté. La nécessité pour les théoriciens de manier des cordes et autres objets dans des espaces possédant un tel nombre de dimensions a créé un formidable terrain de collaboration entre physiciens et mathématiciens. Les recherches dans ce domaine ont eu autant de retombées pour les théories des cordes elles-mêmes que pour diverses branches des mathématiques fondamentales. C'est un bel exemple, dans l'histoire de la physique et des mathématiques, d'une liaison intime entre ces deux disciplines, les résultats de l'une nourrissant les recherches de l'autre. Le jeu en vaut bien la chandelle : bien que les théories des cordes soient encore hautement spéculatives, il ne s'agit rien de moins que de percer les énigmes de l'infiniment petit et de l'infiniment grand, c'est-à-dire, en définitive, celles de nos origines.

Maurice Mashaal
journaliste scientifique

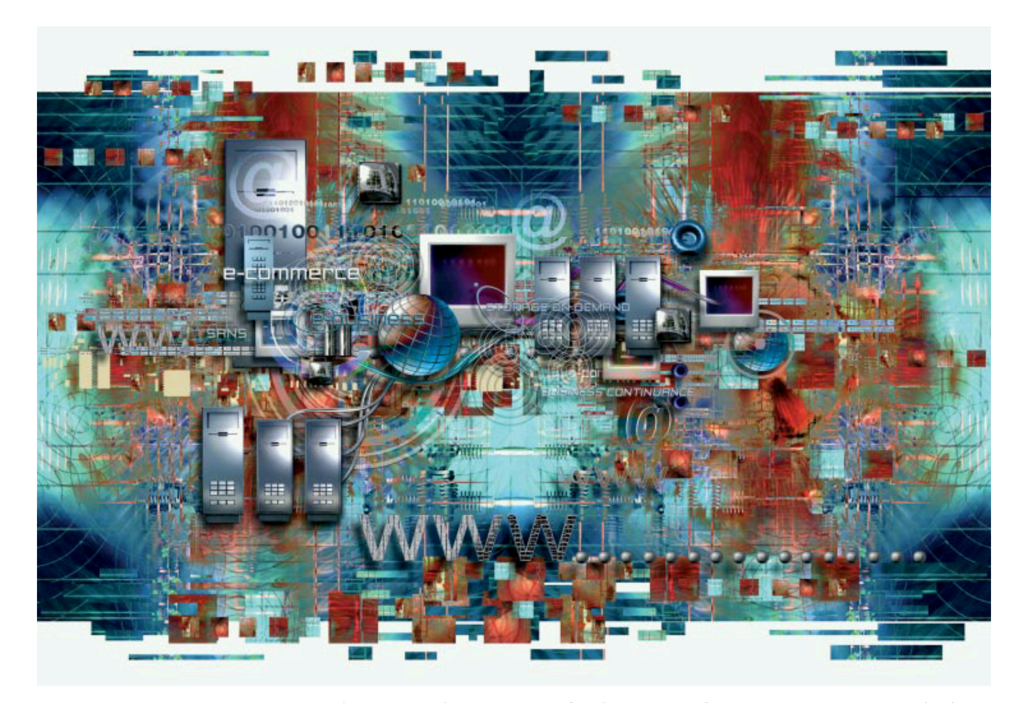
Quelques références :

- B. Greene, *L'Univers élégant* (Robert Laffont, 2000).
- M. Duff, « Les nouvelles théories des cordes », *Pour la Science*, avril 1998.
- N. Arkani-Hamed, S. Dimopoulos, G. Dvali, « Les dimensions cachées de l'Univers », *Pour la Science*, octobre 2000.
- I. Antoniadis, E. Cremmer et K. S. Stelle, « Les supercordes », *Gazette des mathématiciens* n° 87, pp. 17-39, et n° 88, pp. 95-114 (janvier et avril 2001).
- P. Deligne et al. (eds.), *Quantum fields and strings : a course for mathematicians* (American Mathematical Society/Institute for Advanced Study, 1999).

Internet : modéliser le trafic pour mieux le gérer

François Baccelli

Les spécialistes des réseaux de communication s'efforcent de bien comprendre les propriétés statistiques du trafic de données qu'ils doivent acheminer. La gestion de ces réseaux et leur développement en dépendent.



Le réseau Internet n'est pas centralisé comme l'étaient autrefois les réseaux de communication. De tels changements structurels ont des répercussions profondes sur les propriétés mathématiques du trafic de données. (Photo : Getty Images)

Les réseaux de communication (téléphone, Internet, réseaux locaux, etc.) ont connu, au cours des dernières décennies, une expansion phénoménale. Pour leurs opérateurs, une question centrale est de savoir contrôler les flux d'information de façon optimale, afin d'éviter tout engorgement et d'offrir aux utilisateurs un service de bonne qualité, fiable et rapide. Or pour concevoir des procédures efficaces de contrôle de la circulation des informations, pour dimensionner correctement les logiciels et les équipements matériels nécessaires, une connaissance approfondie des propriétés du trafic des communications dans de tels réseaux s'impose.

L'analyse mathématique du trafic dans les réseaux de communication est une discipline déjà ancienne. Elle remonte à 1917, avec les travaux engagés par l'ingénieur danois Agner K. Erlang. Sa démarche, poursuivie par beaucoup d'autres chercheurs, a fourni les principaux outils mathématiques de dimensionnement utilisés par les opérateurs et les constructeurs de réseaux, jusqu'aux années 1990 environ.

Jusqu'aux années 1990, la modélisation du trafic par des lois statistiques classiques suffisait

Dans ses principes, la démarche mathématique explorée par Erlang et par d'autres chercheurs et ingénieurs après lui est *markovienne*. Cela signifie qu'elle décrit le trafic en s'appuyant sur un modèle simple de processus aléatoires, les *chaînes de Markov*, pour lesquelles la théorie mathématique est bien avancée et puissante (Andreï Markov (1856-1922) était un mathématicien russe qui a apporté des contributions importantes à la théorie des probabilités). En simplifiant, une chaîne de Markov est une suite d'événements aléatoires, dans laquelle la probabilité d'un événement donné ne dépend que de l'événement qui précède immédiatement. Dans le cadre des réseaux de communication, la démarche markovienne d'Erlang suppose que les lois statistiques caractérisant le trafic sont des lois de Poisson ; la loi de Poisson est une des lois de probabilité ou de statistique les plus répandues et les plus simples, elle tire son nom du mathématicien français Denis Poisson (1781-1840). L'hypothèse poissonienne s'avérait justifiée pour le trafic téléphonique (où les événements aléatoires sont les appels des abonnés, qui surviennent à des instants aléatoires et dont la durée est également aléatoire).

Ce type de modélisation du trafic a permis de mettre en place des procédures de contrôle adaptées. Jusqu'à une date récente, le contrôle des réseaux de communication était un contrôle d'admission, c'est-à-dire que l'opérateur refuse à l'utilisateur l'accès au réseau lorsque ce dernier ne peut garantir une qualité de service prédéfinie. Ce type de contrôle exige une connaissance assez précise de l'état du réseau dans son ensemble, et il n'est donc possible que pour des réseaux gérés de manière centralisée.

Mais les réseaux de communication d'aujourd'hui ne sont plus ceux d'hier. Internet a connu un développement extraordinaire ces cinq dernières années (on estime que le trafic de communications vocales représentait 90 % du trafic global en 1997, 50 % en 2000, et n'en représentera que 10 % d'ici un an ou deux). Cet essor a radicalement changé une situation qui était stable depuis plus d'un demi-siècle. Les raisons profondes de ce développement rapide résident dans l'utilisation, pour l'acheminement de l'information et le contrôle du trafic, de nouveaux protocoles de routage (routage IP, pour *Internet Protocol*) et de contrôle (TCP, pour *Transmission Control Protocol*) décentralisés, qui rendent le réseau Internet indéfiniment extensible.

Les propriétés statistiques du trafic ont changé. Il fallait comprendre comment et pourquoi

Ces modifications structurelles ont eu des conséquences sur le trafic et ses propriétés statistiques, et il a fallu développer une théorie mathématique adaptée à la nouvelle donne. En effet, des analyses statistiques effectuées au milieu des années 1990 par des chercheurs de Bellcore, aux États-Unis, et de l'INRIA (Institut national de recherche en informatique et en automatique), en France, ont montré, d'abord sur des réseaux locaux puis sur le Web, que le trafic ne pouvait plus être décrit à l'aide de lois de probabilité de Poisson. Notamment, on observe des processus aléatoires à *mémoire longue* (où la probabilité d'un événement dépend aussi d'événements qui se sont pro-

duits relativement loin dans le passé), ce qui exclut toute modélisation usuelle fondée sur les processus markoviens classiques. Souvent, ces processus présentent également des propriétés statistiques connues sous le nom de multi-fractalité, qui traduisent une très grande irrégularité. Or toutes ces propriétés statistiques ont des conséquences importantes, par exemple pour le dimensionnement des mémoires des routeurs ; ne pas en tenir compte pourrait conduire à sous-estimer les pertes de paquets d'informations par le réseau et entraîner des dysfonctionnements.

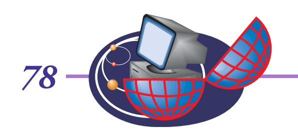


Des internautes dans un cybercafé. Une bonne connaissance des propriétés statistiques des flux de données sur le réseau Internet est indispensable pour assurer le bon fonctionnement de la Toile. (Cliché Frank Moehle)

Depuis les premiers articles mettant en évidence les nouvelles propriétés statistiques du trafic de données, de très nombreux travaux ont été publiés en vue de les expliquer. Aujourd'hui, on comprend assez bien l'origine du phénomène de mémoire longue constaté dans la statistique du trafic. On a pu établir qu'il découle directement de la répartition statistique des tailles de fichiers contenus dans les serveurs Web et FTP (protocole de transfert de fichiers) ainsi que des tailles des fichiers demandés par les utilisateurs lors des requêtes HTTP (protocole de transfert hypertexte, utilisé lorsqu'on surfe sur le Web) et FTP. Leurs courbes statistiques, c'est-à-dire les courbes représentant le nombre de fichiers échangés ou consultés en fonction de la taille, décroissent, pour les grandes valeurs, moins rapidement qu'une exponentielle, de part et d'autre de leur maximum : on dit que leur loi de probabilité est sous-exponentielle. Ce que l'on a montré, c'est que les lois statistiques sous-exponentielles auxquelles obéit le comportement individuel des internautes, superposées en grand nombre étant donnée la multitude de ces internautes, ont pour conséquence directe le phénomène de mémoire longue caractérisant le trafic global.

Analyser le protocole TCP et ses effets afin d'améliorer la gestion du réseau Internet

Tout n'est pas éclairci pour autant. Les travaux actuels se concentrent sur l'explication des propriétés statistiques du trafic aux petites échelles de temps, la multi-fractalité en particulier. L'hypothèse la plus répandue est que cette propriété résulte des protocoles de contrôle utilisés, et notamment de TCP. Mais en quoi consiste le protocole TCP, qui contrôle actuellement près de 90 % du trafic sur Internet ? Il s'agit d'un contrôle de flux adaptatif, où le débit d'information émise par une source est commandé par un algorithme qui



augmente linéairement le débit d'émission au cours du temps, tant qu'il ne se produit pas d'engorgement ; mais dès que des pertes sont détectées, l'algorithme réduit de moitié le débit d'émission.

C'est ce contrôle adaptatif qui règle toute réponse à la congestion dans le réseau. Son analyse mathématique présente de nombreuses difficultés, en raison du caractère décentralisé, stochastique (l'encombrement et les pertes évoluent aléatoirement), non linéaire (les effets ne sont pas simplement proportionnels aux causes), complexe (réseau très étendu, impliquant des interactions entre nombreux routeurs intermédiaires) de la situation. Or l'élaboration de modèles intégrant tous ces éléments est un enjeu majeur, qu'il s'agisse de définir des règles de dimensionnement du réseau, d'optimiser les débits ou de prédire et contrôler les variations aléatoires de la qualité de service offert par le réseau à ses utilisateurs.

Des défis scientifiques et des enjeux économiques, qui mobilisent les universitaires et les industriels

Une telle tâche exige des efforts de recherche dans des domaines très divers (statistiques, théorie des probabilités et des files d'attente, contrôle adaptatif de systèmes non linéaires, théorie des grands réseaux stochastiques, systèmes dynamiques) et qui dépassent ceux de l'approche traditionnelle. Ces dernières années, un grand nombre de modèles plus ou moins simplifiés ont ainsi été proposés. Certains d'entre eux permettent de rendre compte de la multi-fractalité du trafic global, propriété évoquée plus haut, d'autres permettent d'évaluer si le partage d'un même canal de communication entre plusieurs flux de données contrôlés par TCP est équitable, etc.

Les recherches actuelles se concentrent aussi beaucoup sur l'analyse de DiffServ, une méthode de différenciation des services offerts, fondée sur la création de classes de priorité pour les échanges de données. Cela paraît être la seule démarche extensible capable d'améliorer la qualité de service dans le réseau Internet. Un autre axe important concerne l'adaptation d'UDP (User Datagram Protocol), un protocole utilisé pour les flux de données vidéo et vocales, flux qui ne sont pas régulés par TCP, notamment dans le but de définir des modes de transmission de ces flux qui soient compatibles avec TCP.

Face à ces questions qui présentent des défis scientifiques et des enjeux économiques de première importance, le monde académique et le monde industriel s'organisent. Comment ? La plupart des grands groupes industriels des technologies de l'information et des opérateurs ont constitué des équipes de recherche du plus haut niveau, centrées sur la modélisation du trafic et du contrôle dans les réseaux de données, et tout particulièrement dans le réseau Internet. L'effort du monde académique n'est pas moindre, notamment aux États-Unis, en Europe et dans certains pays asiatiques, où se mettent en place des collaborations interdisciplinaires entre des mathématiciens et des chercheurs en informatique ou en génie électrique.

L'instance qui a la plus grande influence dans l'évolution du réseau Internet est sans doute l'IETF (Internet Engineering Task Force, consultable à l'adresse http://www.ietf.org). Elle est ouverte à chacun, qu'il soit concepteur



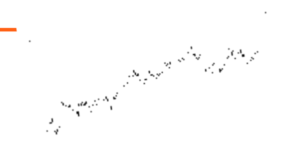
de réseau, chercheur ou opérateur. Les activités se déroulent sous forme de groupes de travail portant sur plusieurs domaines tels que le routage, la sécurité, le transport, le contrôle de congestion, les applications, etc. Ces groupes de travail sont chargés de faire des recommandations dont certaines deviendront des normes. La validation de ces recommandations par des études mathématiques, du type de celles évoquées dans cet article, constitue une composante importante et parfois décisive du travail de normalisation.

François Baccelli
INRIA (Institut national de recherche en informatique et automatique) et
École Normale Supérieure
(Département d'informatique), Paris

Quelques références :

- K. Park et W. Willinger (eds.), *Self similar traffic analysis and performance evaluation* (Wiley, 2000).
- P. Abry, P. Flandrin, M. S. Taqqu et D. Veitch, « Wavelet for the analysis, estimation and synthesis on scaling data », dans la référence ci-dessus.
- F. P. Kelly, A. K. Maulloo et D.K.H. Tan, « Rate control in communication networks : shadow prices, proportional fairness and stability », *Journal of the Operational Research Society, 49*, pp. 237-252 (1998).
- R. Riedi et J. Levy-Vehel, « Fractional brownian motion and data traffic modeling : the other end of the spectrum », *Fractals in Engineering* (Springer-Verlag, 1997).
- M. Taqqu, W. Willinger et R. Sherman, « Proof of a fundamental result in self similar traffic modeling », *Computer Communication Review, 27*, pp. 5-23 (1997).
- F. Baccelli et D. Hong, *Interaction of TCP flows as billiards*, rapport INRIA, avril 2002.

Le prix des options financières



Elyès Jouini

Le monde de la finance fixe le prix des options au moyen de formules ayant été obtenues grâce à des travaux mathématiques relativement récents. La recherche de meilleures formules se poursuit… et cela ne concerne pas que les boursicoteurs!

Dans sa préface à la quatrième édition des *Éléments d'économie politique pure ou théorie de la richesse sociale*, publiée à Lausanne en 1900, Léon Walras écrivait : « *Toute cette théorie est une théorie mathématique, c'est-à-dire que si l'exposition peut s'en faire dans le langage ordinaire, la démonstration doit s'en faire mathématiquement* ». Plus loin, il ajoutait même : « *Il est à présent bien certain que l'économie politique est, comme l'astronomie, comme la mécanique, une science à la fois expérimentale et rationnelle… Le* XX*e siècle, qui n'est pas loin, sentira le besoin […] de remettre les sciences sociales aux mains d'hommes d'une culture générale, habitués à manier à la fois l'induction et la déduction, le raisonnement et l'expérience. Alors l'économie mathématique prendra son rang à côté de l'astronomie et de la mécanique mathématique* ».



La Bourse de New York, un jour faste. Les mathématiques ont fait une entrée en force dans le monde de la finance depuis plus d'une vingtaine d'années. Réciproquement, le monde de la finance fournit des problèmes qui stimulent la recherche dans certains domaines des mathématiques. (Cliché Gamma Liaison/Gifford)

Je voudrais à travers l'exemple qui suit, emprunté à la finance, montrer comment mathématiques et économie continuent d'entretenir des liens extrêmement étroits et qu'il y a, dans les sujets les plus actuels intéressant l'une et l'autre discipline, une réelle fertilisation croisée.

Le problème qui va nous intéresser ici est l'évaluation des options financières. La question est aussi vieille que les options elles-mêmes, dont on trouve notamment trace dans l'Antiquité et au XVIIe siècle sur le marché des tulipes aux Pays-Bas. C'est pourtant en 1973, comme on le verra plus loin, que cette question a trouvé sa première réponse mathématiquement satisfaisante. Et ce n'est pas un hasard si c'est la même année que le premier marché organisé d'options, celui de Chicago, a connu un essor jamais démenti depuis.

Qu'est-ce qu'une option financière ? Considérons une certaine action cotée sur les marchés financiers, et dont le prix est, aujourd'hui, égal à *S*. Les marchés financiers offrent aux acheteurs potentiels, par le biais d'une *option*, la possibilité d'acheter cette action à une date ultérieure, mettons dans trois mois, au prix *K*. Cela peut être intéressant pour un acheteur qui, par exemple, ne dispose pas encore de l'argent nécessaire et veut se garantir contre une augmentation du prix de l'action. Une telle option est une sorte de contrat d'assurance, qui confère le droit d'acheter l'action à une date ultérieure à un prix garanti *K*. Évidemment, ce droit doit lui-même être vendu à un certain prix, mais lequel ? Telle est la question de l'évaluation du prix des options. Pour parler en termes financiers : quel doit être le prix d'une option sur l'action *S*, de « strike » ou prix d'exercice *K* et d'échéance trois mois ?

Il est clair que l'acheteur d'un tel droit ne l'exercera que si, dans trois mois, le prix de l'action sur le marché est supérieur à *K*. Il pourra alors acheter l'action au prix *K*, revendre au prix courant et réaliser un bénéfice égal à la différence. Cette option procure donc à son acheteur, dans trois mois, un gain égal à la différence entre le prix courant de l'action et *K*, si cette différence est positive, et un gain nul sinon.

Le principe de non-arbitrage est à la base de la détermination des prix des actifs financiers

Pour fixer le prix d'une telle option, la théorie de l'arbitrage s'appuie sur un principe très simple, voire simpliste : l'absence d'opportunités d'arbitrage. En d'autres termes, ce principe affirme qu'il n'est pas possible, à partir d'un investissement nul aujourd'hui, de se garantir, quoi qu'il arrive, un paiement positif à une date ultérieure (on n'a rien pour rien). Le principe d'absence d'opportunités d'arbitrage ne signifie pas que des gains miraculeux soient impossibles. En effet, je peux très bien emprunter le prix d'un billet de loterie et acheter un tel billet — mon apport personnel est donc nul — puis gagner un million d'euros, rembourser mon emprunt et dégager un bénéfice énorme. Le principe énonce seulement qu'un tel bénéfice ne saurait être garanti *a priori*. En effet, dans l'opération précédente, je peux également ne rien gagner et être obligé de rembourser mon emprunt : j'ai donc pris un risque de perte.

Ainsi, l'absence d'opportunités d'arbitrage signifie tout simplement que tout gain supérieur au rendement d'un actif sans risque de référence (taux d'intérêts, obligations, bons du Trésor, etc.) est nécessairement lié à un risque. Les SICAV, par exemple, ont un rendement moyen supérieur à celui du marché monétaire ; toutefois, ce rendement n'est pas garanti et peut très bien, comme nous l'avons vu au cours de l'année 2001, passer en dessous de celui du marché monétaire.

Supposons à présent, pour simplifier le problème, que le marché ne fonctionne qu'à deux dates, aujourd'hui et dans trois mois, et que le prix *S* de l'action dans trois mois ne pourra prendre que deux valeurs, disons soit 100 soit 150 euros. Supposons de plus que *K*, le prix d'achat convenu pour l'action à l'échéance de l'option, soit compris entre la valeur haute S_h = 150 euros et la valeur basse S_b = 100 euros, par exemple *K* = 140 euros. Si le prix de l'action dans trois mois est la valeur haute 150 euros, le détenteur de l'option exerce son droit et l'achète au prix préalablement convenu *K* = 140 euros; le gain associé à l'option vaut donc $S_h - K = 150 - 140 = 10$ euros. Si le prix de l'action dans trois mois est la valeur basse 100 euros, le détenteur de l'option renonce à exercer son droit d'achat au prix *K*, qui est supérieur; le gain associé à l'option est, dans ce cas, nul.

On peut démontrer qu'un tel gain peut également être obtenu en se constituant un portefeuille ne comportant que des actions et des placements (ou prêts) sur le taux d'intérêt du marché, que l'on notera ici *r*. Appelons *C* le coût de constitution d'un tel portefeuille. Deux actifs aux rendements identiques devant avoir le même prix (on prouve que sinon, le principe de non-arbitrage serait violé), on en conclut que le prix de l'option doit être égal à *C*.

Le coût *C* du portefeuille, égal à celui de l'option, peut être déterminé de façon précise. On démontre que *C* est une moyenne pondérée des paiements actualisés de l'option, c'est-à-dire une moyenne pondérée des montants $(S_h - K)/(1 + r)$ et $0/(1 + r) = 0$, et que les poids intervenant dans cette moyenne sont tels que le prix *S* de l'action aujourd'hui est, lui-même, une moyenne pondérée des paiements actualisés de l'action ($S_h/(1 + r)$ et $S_b/(1 + r)$) avec les mêmes poids. Plus précisément, on prouve qu'il existe une loi de probabilité telle que le prix de tout actif est égal à l'espérance, calculée d'après cette loi, de ses paiements actualisés futurs. Ce dernier résultat est obtenu grâce à de l'algèbre linéaire élémentaire, et concerne le modèle simple présenté ci-dessus. Mais grâce à des techniques d'*analyse convexe* apparues au milieu du XXe siècle, il se généralise au cas où l'action peut prendre plusieurs valeurs différentes (en nombre fini).

Le calcul stochastique : quand finance et mathématiques théoriques s'enrichissent mutuellement

Cependant, si l'on souhaite adhérer davantage à la réalité et considérer un modèle en temps continu et avec un continuum de prix possibles, il faut alors, pour interpréter le même principe simple d'arbitrage, faire appel à des notions plus avancées de la théorie des probabilités, apparues dans la deuxième moitié du XXe siècle. Il s'agit plus précisément de la théorie des processus stochastiques (processus où des quantités évoluent aléatoirement au cours du temps) et la théorie des équations différentielles stochastiques (équations différentielles où interviennent des quantités aléatoires). Dans ces domaines, les développements les plus récents sont étroitement liés aux problèmes rencontrés en finance.

Ces modèles supposent que le cours de l'action évolue avec un taux de rendement déterministe (non aléatoire), auquel s'ajoute un terme aléatoire de moyenne nulle et d'amplitude propre à l'actif considéré. Cette fluctuation aléatoire est appelée *volatilité* et peut dépendre du temps et de nombreux autres événements endogènes ou exogènes.

Moyennant ces hypothèses, on trouve que le prix de l'option obéit à une certaine équation aux dérivées partielles (équation différentielle où la fonction inconnue dépend de plusieurs variables). Dans le cas le plus simple, étudié indépendamment par les Américains Fischer Black et Myron Scholes d'une part et Robert Merton d'autre part en 1973, cette équation est la même que l'équation de diffusion de la chaleur, bien connue des physiciens. Il est alors possible de la résoudre explicitement et de déterminer le prix de l'option en fonction de ses propres caractéristiques (échéance, prix d'exercice) ainsi que du cours de l'action et de sa volatilité : c'est la formule de Black-Scholes et Merton, qui a valu à Scholes et Merton le prix Nobel d'économie en 1997 (Black est décédé en 1995).

Cette formule et ses variantes sont utilisées dans toutes les places financières du monde. Programmées sur tous les ordinateurs des salles de marché, mises à contribution d'innombrables fois par jour, elles sont l'exemple même du lien possible entre mathématiques théoriques et applications concrètes. La formule de Black-Scholes et Merton ne correspond cependant qu'au cas simpliste où taux d'intérêts, taux de rendements moyens, niveaux de risque, etc., demeureraient constants au cours du temps. Dès que l'on modifie ces hypothèses, les équations obtenues ne sont plus équivalentes à celle de la diffusion de la chaleur. Les équations pertinentes en sont des variantes, et elles nécessitent le plus souvent des méthodes de résolution — implicites, explicites ou numériques — spécifiques. C'est en travaillant sur certaines de ces équations que les chercheurs français C. Daher et M. Romano, qui travaillaient à l'époque à l'université Paris-Dauphine et à la Caisse autonome de refinancement, ont obtenu en 1990 le prix IBM de calcul numérique intensif.

Enfin, lorsqu'on essaye d'être plus réaliste et de prendre en compte les coûts de transaction, les diverses contraintes imposées par le marché ou encore l'impact du nombre des transactions sur les prix, les techniques du calcul stochastique classique ne suffisent plus. Il faut développer, comme cela a été fait ces dernières années, des outils spécifiques comme les *équations différentielles stochastiques rétrogrades* ou des méthodes fines de *dualité* en *contrôle optimal stochastique*. On découvre alors, et cela peut surprendre, que ces nouvelles idées mathématiques, développées pour résoudre des problèmes économiques et financiers, s'avèrent liées à des problèmes déjà rencontrés en géométrie ou en physique — par exemple la déformation de surfaces ou la fonte de glaçons — et qu'elles éclairent ces derniers d'un jour nouveau.

Elyès Jouini
Professeur des Universités, CEREMADE (Centre de mathématiques de la décision)
Université Paris-Dauphine (Paris 9)

Quelques références :

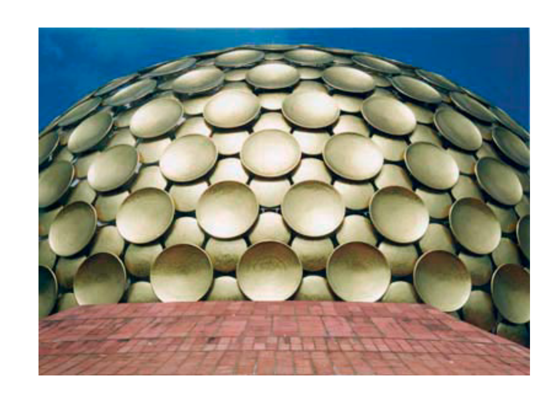
- N. Bouleau, *Martingales et marchés financiers* (Odile Jacob, 1998).
- F. Black et M. Scholes, « The pricing of options and corporate liabilities », *Journal of Political Economy, 81*, pp. 637-654 (1973).
- C. Huang et R. Litzenberger, Foundations for financial economics (North-Holland, 1988).
- L. Walras, *Éléments d'économie politique pure ou théorie de la richesse sociale* (Corbaz, Lausanne, 1874, édition définitive revue et augmentée par l'auteur, LGDJ, Paris, 1952).

Communiquer sans erreurs : les codes correcteurs

Gilles Lachaud

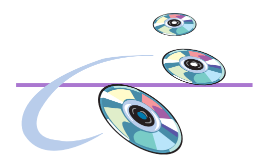
Pour détecter et corriger les inévitables erreurs qui affectent les échanges d'information numérisée, les spécialistes du codage en appellent à des méthodes abstraites qui relèvent de l'algèbre ou de la géométrie.

Nous sommes en pleine ère numérique. Qu'est-ce que cela veut dire ? Tout simplement qu'une partie énorme des informations échangées à travers la planète est matériellement représentée sous la forme de nombres. Messages électroniques, téléphonie mobile, transactions bancaires, téléguidage de satellites, télétransmission d'images, disques CD ou DVD, etc. : dans tous ces exemples, l'information est traduite — on dit *codée* (à ne pas confondre avec cryptée) — en suites de nombres entiers, et correspondant physiquement à des signaux électriques ou autres. Plus précisément même, l'information est généralement codée sous forme de suites de chiffres binaires — des 0 ou des 1, appelés aussi bits. Par exemple, dans le code ASCII (*American Standard Code for Information Interchange*) utilisé par les micro-ordinateurs, le A majuscule est codé par l'octet (séquence de 8 bits) 01000001, le B majuscule par 01000010, etc.



Le Matrimandir à Auroville (Tamil Nadu, Inde), géode construite par l'architecte français Roger Anger. Dans la conception de codes correcteurs efficaces, on rencontre des problèmes apparentés à des questions difficiles de pure géométrie, comme celui de recouvrir une sphère par le plus grand nombre possible de disques de même taille, sans qu'ils se chevauchent.

Un problème majeur de la transmission de l'information est celui des erreurs. Il suffit d'une petite rayure sur un disque, d'une perturbation de l'appareillage, ou d'un quelconque phénomène parasite pour que le message transmis comporte des erreurs, c'est-à-dire des « 0 » qui ont malencontreusement été changés en « 1 », ou inversement. Or l'un des nombreux atouts du numérique est la possibilité de détecter, et même de corriger, de telles erreurs !



On rallonge les mots du message de façon qu'après dégradation, on puisse quand même les reconnaître

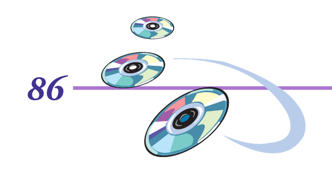
Telle est la fonction des *codes correcteurs d'erreurs*, dont les premiers ont été conçus à la même époque que les premiers ordinateurs, il y a plus d'une cinquantaine d'années. Comment font-ils ? Le principe est le suivant : on allonge les « mots » numériques qui composent le message, de façon qu'une partie des bits servent de bits de contrôle. Par exemple, dans le code ASCII évoqué plus haut, l'un des huit bits est un bit de contrôle : il doit valoir 0 si le nombre de « 1 » dans les 7 autres bits est pair, et 1 sinon. Si l'un des huit bits a inopinément basculé de valeur, la parité indiquée par le bit de contrôle ne correspond plus et une erreur est alors détectée. La même idée se retrouve dans bien des numéros que l'on rencontre dans la vie quotidienne. Par exemple, dans les relevés d'identité bancaire, on ajoute une lettre-clé à un numéro de compte pour pouvoir détecter une erreur de transmission. De même, les numéros des billets de banque en euros sont codés pour éviter les contrefaçons. Autrement dit, la philosophie des codes correcteurs est de composer des messages *redondants* : chaque mot du message est allongé de façon à contenir une information sur le message lui-même !

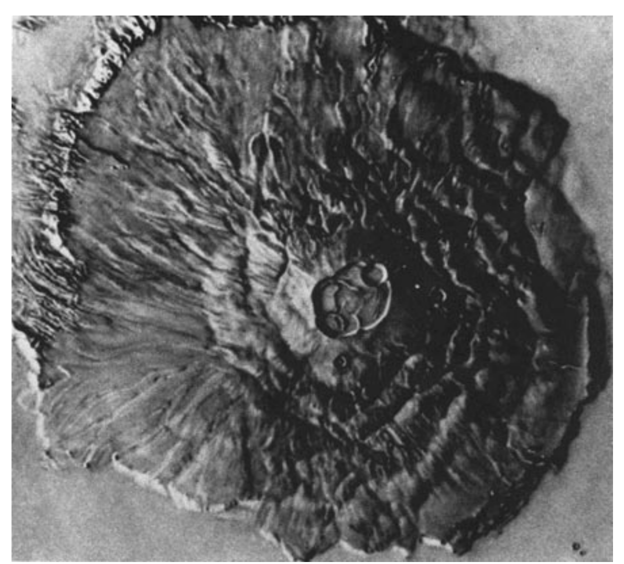
Un exemple simple et éclairant, mais peu réaliste, de code correcteur d'erreurs est la triple répétition : chaque bit du message à coder est triplé, c'est-à-dire que 0 devient 000 et 1 devient 111. Ce code permet de détecter et corriger une erreur éventuelle sur un triplet. En effet, si l'on reçoit, mettons, la séquence 101, on en déduit immédiatement que la bonne séquence était 111 (on suppose qu'un seul bit sur les trois reçus est erroné), et donc que l'information initiale était le bit 1. Le code de triple répétition n'est pas réaliste car il est coûteux : pour chaque bit d'information, il faut en envoyer trois ; on dit que son taux de rentabilité est 1/3. Ce taux a des répercussions directes sur la durée nécessaire à la transmission des messages et sur le coût des communications.

Un bon code correcteur doit posséder d'autres qualités en plus d'un taux de rentabilité élevé. Il lui faut également une bonne capacité de détection et correction d'erreurs, et la procédure de décodage doit être suffisamment simple et rapide. Tout le problème de la théorie des codes correcteurs d'erreurs est là : construire des codes qui détectent et corrigent le plus possible d'erreurs, tout en allongeant le moins possible les messages, et qui soient faciles à décoder.

L'algèbre des corps finis s'applique naturellement aux codes, car ceux-ci utilisent un alphabet fini

Les mathématiques interviennent depuis longtemps dans ces questions. Déjà en 1948, le mathématicien américain Claude Shannon, un des pères de la théorie de l'information, obtenait des résultats théoriques généraux affirmant qu'il existe des codes ayant des qualités optimales, en un sens technique précis. Cependant, si le théorème de Shannon établissait l'existence de très bon codes correcteurs, il ne fournissait pas de méthode pratique pour les construire. Par ailleurs, on disposait de codes correcteurs aux performances modestes, comme les codes de Hamming, du nom de leur inventeur, le mathématicien américain Richard





Olympus Mons, sur la planète Mars, est le plus grand volcan du système solaire : environ 600 km de diamètre et 27 km de hauteur ! Cette image a été obtenue grâce à la sonde spatiale Mariner 9, en 1971-1972. La sonde envoyait à la Terre ses informations en utilisant un code correcteur capable de corriger jusqu'à 7 bits erronés sur 32. Dans chaque groupe de 32 bits, 26 étaient des bits de contrôle, et les 6 autres constituaient l'information nette. Aujourd'hui, on dispose de codes correcteurs encore plus performants. (Cliché NASA/JPL)

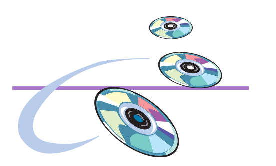
W. Hamming (1915-1998), dans les années 1950 (dans ces codes, qui ont été beaucoup utilisés, les bits de contrôle sont déterminés en fonction des bits d'information par des équations linéaires simples).

Les spécialistes se sont alors mis à étudier de manière systématique les codes correcteurs et leurs propriétés, dans le but d'obtenir concrètement des codes aussi performants ou presque que le prédisaient les résultats théoriques de Shannon. Pour ce faire, ils ont utilisé à fond l'algèbre. Si le codage de l'information se fait directement dans l'« alphabet » binaire 0 et 1, l'algèbre sous-jacente est celle du pair et de l'impair, connue déjà de Platon (pair + pair = pair, pair + impair = impair, pair x pair = pair, impair x impair = impair, etc.). En fait, il s'avère plus intéressant de considérer des « alphabets » de codage ayant plus de deux chiffres, et de traduire seulement à la fin de la procédure le résultat en suites binaires de 0 et 1. Comme un alphabet comporte un nombre fini de symboles, et que l'on souhaite effectuer des calculs sur ces symboles, l'algèbre sous-jacente est l'objet de la *théorie des corps finis*, créée par le jeune mathématicien français Évariste Galois au début du XIXe siècle, en étudiant la résolubilité des équations algébriques (un corps fini est un ensemble d'éléments en nombre fini qui peuvent s'additionner, se multiplier et se diviser de manière analogue aux nombres ordinaires, le résultat des opérations restant à l'intérieur de cet ensemble. L'ensemble constitué par 0 et 1, avec les règles arithmétiques du pair et de l'impair, est le corps fini à deux éléments ; c'est le corps fini le plus simple).

Ainsi, c'est à l'aide d'algèbre abstraite et élaborée, en liaison avec la théorie des corps finis, qu'ont été construits des codes correcteurs d'erreurs très efficaces, adaptés à tel ou tel type de transmission d'information. Deux exemples parmi une multitude d'autres sont le code employé pour la gravure des disques audionumériques (il permet de corriger jus-



Quoi qu'en dise ce timbre français émis en 1984, Évariste Galois n'était pas un géomètre mais un algébriste. C'était le pionnier de la théorie des groupes, ainsi que de la théorie des corps finis utilisée notamment par les spécialistes des codes correcteurs d'erreurs. Provoqué en duel, Galois est mort à l'âge de 21 ans à peine.



qu'à environ 4 000 bits erronés consécutifs, l'équivalent d'une rayure sur plus de 2 millimètres de piste !), et celui qu'a utilisé la sonde spatiale Mariner 9 pour nous envoyer ses images de la planète Mars.

Une nouvelle famille de codes faisant appel à la géométrie algébrique des courbes

L'algèbre abstraite n'est pas le seul instrument dont disposent les spécialistes des codes correcteurs. Il y a aussi la géométrie, et plus particulièrement la géométrie algébrique. Celle-ci, très vaste partie des mathématiques actuelles, a pour point de départ l'étude des objets géométriques — courbes, surfaces, etc. — définis par des équations algébriques. Tout lycéen sait par exemple qu'une parabole peut être représentée par une équation algébrique, de type $y = ax^2 + bx + c$, où x et y sont les coordonnées des points de la parabole. On peut aussi étudier des courbes définies sur des corps finis, c'est-à-dire que dans les équations algébriques qui les représentent, les grandeurs comme x et y ne sont pas n'importe quels nombres, mais uniquement des éléments d'un certain corps fini. En utilisant de telles courbes et l'algèbre associée aux coordonnées de leurs points (qui sont en nombre fini), on a inauguré, il y a environ vingt ans, une nouvelle famille de codes correcteurs : les codes géométriques. Cela a permis récemment d'obtenir de nouveaux résultats concernant les codes binaires, et de construire des codes encore plus performants que ceux prédits par les travaux de Shannon. En contrepartie, l'analyse des codes géométriques a conduit les mathématiciens à examiner de plus près le nombre de points d'une courbe algébrique définie sur un corps fini. On a là un bel exemple de la rétroaction positive qu'un domaine d'application peut exercer sur la discipline théorique dont il se sert.

Gilles Lachaud
Institut de mathématiques de Luminy, CNRS, Marseille

Quelques références :

- P. Arnoux, « Codage et mathématiques », *La science au présent* (édition Encyclopædia Universalis, 1992).
- P. Arnoux, « Minitel, codage et corps finis », *Pour la Science* (mars 1988).
- G. Lachaud et S. Vladut, « Les codes correcteurs d'erreurs », *La Recherche* (juillet-août 1995).
- O. Papini, « Disque compact : « la théorie, c'est pratique ! » dans « Secrets de nombres », Hors-série n° 6 de la revue *Tangente* (1998).
- O. Papini et J. Wolfmann, *Algèbre discrète et codes correcteurs* (Springer-Verlag, 1995).
- J. Vélu, *Méthodes mathématiques pour l'informatique* (Dunod, 1995).
- M. Demazure, *Cours d'algèbre — primalité, divisibilité, codes* (Cassini, 1997)

Reconstruire des surfaces pour l'imagerie

Jean-Daniel Boissonnat

Reconstituer une surface en ne connaissant que certains de ses points : un problème que l'on rencontre souvent, qu'il s'agisse d'exploration géologique, d'archivage de vestiges archéologiques, d'imagerie médicale ou industrielle.

Lorsqu'on sonde le sous-sol en certains endroits pour connaître la configuration des différentes couches géologiques, ou lorsqu'on veut cartographier un fond marin, le nombre de points de mesure est nécessairement fini. Or il faut reconstruire, à partir de ces données en nombre restreint, les surfaces correspondantes. La situation est analogue avec tous les systèmes d'imagerie informatisés (scanners, télémètres, imageurs tridimensionnels, etc.) utilisés en médecine, dans l'industrie, en archéologie, etc. Comme point de départ, il y a un objet réel — qui peut être une partie du corps humain, une pièce mécanique, un vestige archéologique, une structure géologique, ou autre. De cet objet réel, les instruments ne peuvent enregistrer que certains points, à partir desquels on doit reconstruire virtuellement la forme de l'objet. Tel est le problème dit de la reconstruction de surfaces (Figure 1). Il consiste donc à exploiter un nombre fini de points pour fournir une représentation géométrique et informatique de l'objet, ce qui permettra de le visualiser sur un écran, de l'ar-



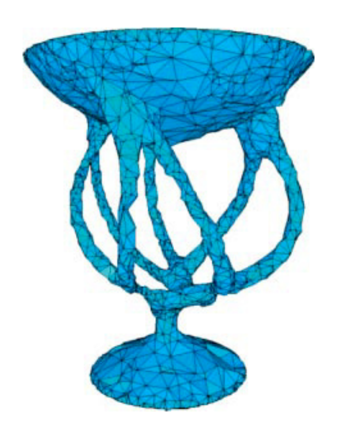




Figure 1. La reconstruction d'une surface à partir d'un échantillon de ses points : ce problème se pose dans des domaines variés .

chiver dans la mémoire de l'ordinateur, de procéder aisément à des calculs, voire de modifier l'objet ou d'en télécommander l'usinage d'une copie. Bref, une fois que la forme d'un objet réel est numériquement enregistrée, et ce avec suffisamment de précision, on dispose de maintes possibilités d'action et de calcul.

Les enjeux économique et industriel du problème de la reconstruction de surfaces, son caractère fondamental du point de vue scientifique, ont conduit à de nombreux travaux depuis une vingtaine d'années. Mais ce n'est que très récemment que les spécialistes ont formalisé en termes mathématiques le problème, ce qui leur a permis de concevoir des algorithmes efficaces et fournissant une reconstruction fidèle. Le transfert vers l'industrie de certains de ces résultats de géométrie dite algorithmique s'est alors opéré de manière très rapide au travers de la création de jeunes pousses (comme *Raindrop Geomagic* aux États-Unis) ou le lancement de nouveaux produits par les leaders de la conception assistée par ordinateur ou de l'imagerie médicale (*Dassault Systèmes, Siemens Medical*).

Diagrammes de Voronoï et triangulation de Delaunay, deux outils géométriques indispensables

Pour reconstruire une surface à partir d'un nuage de points qui l'échantillonnent, la grande majorité des algorithmes utilisent un outil central en géométrie algorithmique : la triangulation de Delaunay, nommée d'après Boris Delone (1890-1980), mathématicien russe dont le nom a été francisé en Delaunay. La triangulation de Delaunay se définit naturellement à partir de ce qu'on appelle le *diagramme de Voronoï*, du nom du mathématicien russe Georgi Voronoï (1868-1908). Considérons un ensemble fini de points dans l'espace, et appelons-le *E*. Le diagramme de Voronoï de *E* est une division de l'espace en cellules convexes (en bleu sur la Figure 2), où chaque cellule est constituée des points de l'espace plus proches d'un point de *E* que des autres points de *E*. Les cellules — ce sont des polyèdres convexes — sont ainsi définies de manière univoque.

Maintenant, relions par des segments de droite les points de *E* dont les cellules de Voronoï sont adjacentes. L'ensemble de ces segments constitue la *triangulation de Delaunay* (en vert sur la Figure 2) associée à *E*. Ces structures se définissent dans des espaces de dimension quelconque ; c'est le cas de la dimension trois — l'espace usuel — qui est le plus intéressant pour la reconstruction de surfaces. Les diagrammes de Voronoï (Figures 2 et 3) figurent parmi les principaux

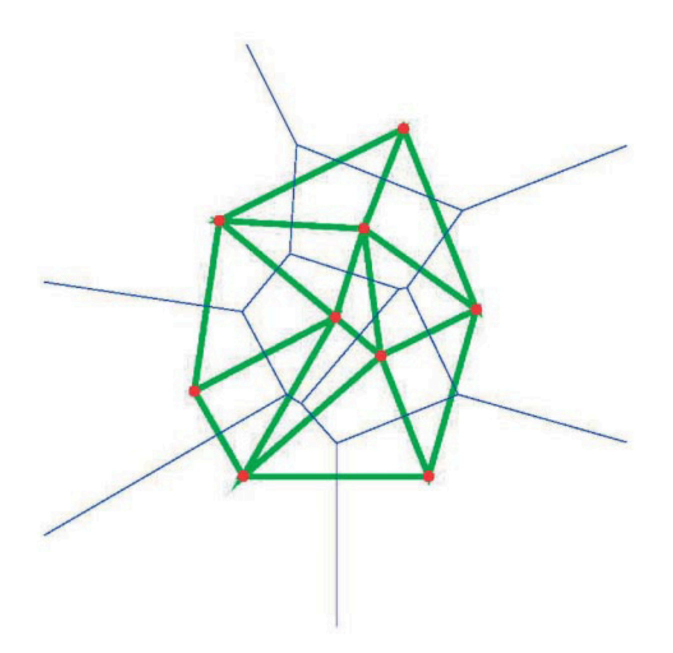


Figure 2. Le diagramme de Voronoï (en bleu) et la triangulation de Delaunay (en vert) d'un ensemble de points (marqués en rouge). Le diagramme de Voronoï et la triangulation de Delaunay sont des outils fondamentaux en géométrie algorithmique.

sujets d'étude de la géométrie algorithmique, et c'est dans les années 1980 que l'on a établi leur lien avec la théorie des polytopes (analogues des polyèdres dans les espaces de dimension supérieure à trois). Leur étude dans le contexte de l'échantillonnage des surfaces est beaucoup plus récente.

Quel est l'intérêt des diagrammes de Voronoï et des triangulations de Delaunay ? Si *E* est un échantillon de *n* points pris sur une surface *S*, on peut montrer que son diagramme de Voronoï et la triangulation de Delaunay correspondante contiennent beaucoup d'informations sur cette surface. Lorsque l'échantillonnage est suffisamment dense, on peut fournir des approximations précises de la surface. Par exemple, le vecteur qui joint un point P de *E* au sommet le plus éloigné de sa cellule de Voronoï est une bonne approximation de la normale à la surface *S* au point P.

Il faut s'assurer que les temps de calcul resteront raisonnables, que les algorithmes sont fiables

C'est ainsi que l'on connaît aujourd'hui plusieurs algorithmes de reconstruction capables, à partir d'un échantillon fini de points d'une surface S, de construire une surface *S'* qui approxime correctement la surface réelle *S*. Qui plus est, la théorie de ces algorithmes permet de calculer une borne supérieure sur la différence entre *S'* et *S*, borne qui dépend évidemment de la densité d'échantillonnage.

Comme les jeux de données fournis par les instruments de mesure comportent généralement plusieurs centaines de milliers de points, voire des millions, les questions combinatoires et algorithmiques jouent un rôle critique. Il est par exemple important de savoir si la quantité de calculs que nécessite la triangulation de Delaunay restera ou non dans une limite raisonnable. Dans les cas les plus défavorables, le nombre *T* d'étapes de calcul (c'est-à-dire, en fin de compte, le temps de calcul) peut être quadratique ; autrement dit, *T* est au pire proportionnel au carré du nombre de points de l'échantillonnage. On suppose toutefois que cette situation ne se produit pas dans le cas de surfaces bien échantillonnées. Des résultats plus précis ont été démontrés très récemment dans le cas de surfaces *S* polyédriques, c'est-à-dire constituées uniquement de facettes polygonales : pour de telles surfaces et pour des conditions d'échantillonnage faibles, la taille du calcul de triangulation est, au pire, proportionnelle au nombre de points échantillonnés. Le cas des surfaces lisses est plus délicat ; il fait actuellement l'objet de recherches actives.

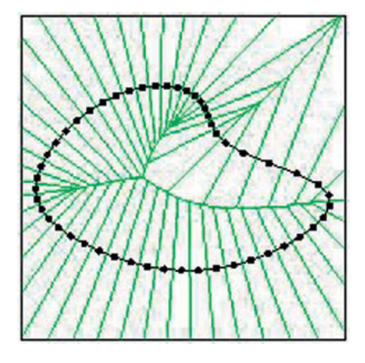


Figure 3. Le diagramme de Voronoï d'un ensemble de points pris sur une courbe.

Les bornes théoriques ne sont pas tout, reste à savoir calculer effectivement et rapidement la triangulation d'un jeu de données. On connaît de nombreux algorithmes. Les plus efficaces sont dits randomisés car ils effectuent certains tirages aléatoires au cours de leur déroulement. La théorie des algorithmes randomisés s'est développée très rapidement dans

les années 1990 et a conduit à des analyses précises, validées expérimentalement. Dans bien des cas, et le calcul de la triangulation de Delaunay en est un, l'introduction d'une part de hasard autorise à ne pas chercher à résoudre de manière optimale le cas le pire (qui est peu probable) et conduit à des algorithmes simples et très efficaces en moyenne. On sait ainsi traiter des échantillons de 100 000 points en une dizaine de secondes (Pentium III à 500 MHz).

Si calculer vite est important, calculer de manière fiable l'est encore plus. Cette question est délicate, car les ordinateurs ne savent généralement représenter les nombres qu'avec une précision finie (un nombre fini de décimales). Ainsi, il est impossible de donner une représentation à la fois numérique et exacte de nombres comme π ou √2, qui comportent une infinité de décimales. L'accumulation des erreurs d'arrondis peut alors conduire à un comportement anormal des programmes. Si ces comportements sont bien connus, ils sont difficiles à maîtriser, et la réalisation et la maintenance d'algorithmes fiables sont très coûteuses. Une part importante de la recherche récente en géométrie algorithmique porte sur ces questions et mêlent algorithmique, calcul formel (où l'ordinateur manipule des symboles, et non des nombres explicites) et arithmétique des ordinateurs. Elles ont d'ores et déjà débouché sur le développement de bibliothèques de logiciels permettant une programmation facile, efficace et sûre, telle que la bibliothèque CGAL (*Computational Geometry Algorithms Library*) développée par une collaboration internationale d'universités et d'organismes de recherche.

Jean-Daniel Boissonnat
INRIA (Institut national de recherche en informatique et en automatique), Sophia-Antipolis

Quelques références :

- J.-D. Boissonnat et M. Yvinec, *Algorithmic geometry* (Cambridge University Press, 1998).
- J.-D. Boissonnat et F. Cazals, « Smooth surface reconstruction via natural neighbour interpolation of distance functions », dans *Proceedings of the 16th Annual ACM Symposium of Computational Geometry* (2000).
- CGAL, The Computational Geometry Algorithms Library, http://www.cgal.org.

Les mathématiciens en France et dans le monde

Jean-Pierre Bourguignon

Jusque vers la fin du XIXe siècle, les « géomètres », comme on appelait jadis les mathématiciens, étaient peu nombreux. En un siècle, leurs rangs se sont considérablement renforcés. Aujourd'hui, ils doivent faire face à une profonde mutation de leur discipline.

Au cours du XXe siècle, la communauté mathématique a connu une expansion numérique majeure. Elle est passée de quelques centaines de membres en 1900 à des dizaines de milliers (probablement de l'ordre de 80 000) 100 ans plus tard. Pour faire une estimation de ce genre, il faut d'abord que l'on s'entende sur la définition du terme « mathématicien ». Nous réservons ce nom à ceux et celles ayant atteint un niveau de formation équivalent à la thèse de doctorat, et dont la profession accorde une place véritable à la recherche mathématique ou à l'assimilation de ses résultats. Ce choix peut être jugé un peu limitatif car il a par exemple pour effet d'exclure de notre champ de vision presque tous les professeurs de l'enseignement secondaire — une catégorie dont le nombre a aussi augmenté considérablement dans tous les pays du monde au cours de la deuxième moitié du XXe siècle.

Cette croissance résulte de plusieurs processus simultanés. Il y a eu tout d'abord, juste après la Deuxième guerre mondiale, une prise de conscience de l'importance des sciences dans le développement économique ou industriel. Par ailleurs, de nouveaux groupes de personnes ont accédé à ces professions. Il en est ainsi des femmes, certes avec de grandes inégalités d'un pays à l'autre. Mais dans le même temps, une communauté académique, regroupant les acteurs de l'enseignement supérieur, a fait son apparition dans presque tous les pays. Pour ne donner qu'un exemple, les mathématiciens originaires d'Afrique sub-saharienne ont soutenu leurs premières thèses de doctorat dans les années 1970, après formation dans une université d'un pays occidental ou en Union soviétique. La génération suivante a souvent fait ses études sur place : dans la décennie 1990-2000, de nombreux pays d'Afrique sub-saharienne ont mis en place des formations supérieures autonomes et ont, de ce point de vue, accédé à l'indépendance. Dans les prochaines années, l'expansion va continuer avec probablement un renforcement considérable des communautés mathématiques d'autres pays, comme la Chine et l'Inde.



La Terre vue de nuit. La répartition mondiale des lumières nocturnes n'est pas sans rappeler celle des centres d'activité mathématique. Pour autant, les mathématiciens ne travaillent pas tous la nuit ! (Cliché C. Mayhew et R. Simmon/NASA-GSFC)

Une communauté de chercheurs et son réseau de sociétés savantes

Comment les communautés de mathématiciens sont-elles organisées ? L'expansion de la communauté mathématique internationale a été accompagnée d'une structuration par le biais de sociétés savantes, qui vivent presque toutes grâce au dévouement et à l'engagement de collègues bénévoles. Les sociétés de mathématiques sont aujourd'hui encore de taille modeste, à l'exception de *l'American Mathematical Society* qui regroupe près de 15 000 membres et qui a plus de 200 employés.

La première étape s'est produite au niveau national, le plus souvent à un moment où les pouvoirs publics ont perçu que le développement des sciences pouvait représenter un enjeu économique et militaire. C'est ainsi que la *Société mathématique de France* (SMF), comme d'ailleurs la *Société française de physique*, est née en 1872, juste après la déroute de 1870 face à l'Allemagne, et la réflexion sur ses causes qui s'en est suivie. Cette perspective étroitement nationaliste s'est, heureusement, estompée.

L'*Union mathématique internationale* a été créée en 1896. Elle est restée une petite structure. Sa responsabilité principale est de fournir le cadre de l'organisation du *Congrès international des mathématiciens*, un événement quadriennal qui demeure le rendez-vous incontournable de la communauté à l'échelle mondiale. Son comité exécutif se charge aussi de nommer la commission qui attribue, tous les quatre ans, les médailles Fields ; celles-ci représentent la récompense la plus prestigieuse en mathématiques, le prix Nobel n'existant pas dans cette discipline.



L'IHÉS (Institut des hautes études scientifiques), à Bures-sur-Yvette en banlieue parisienne, et une discussion entre mathématiciens dans ses locaux. L'IHÉS, consacré aux mathématiques fondamentales et à la physique théorique, est un institut de recherche prestigieux. Il ne compte que 7 chercheurs permanents mais accueille chaque année, pour des durées variables, quelque 200 chercheurs de toutes nationalités. Récemment, quelques-uns de ses mathématiciens ont commencé à se pencher sur des problèmes liés à la biologie moléculaire. (Clichés IHÉS et IHÉS-Outsider Agency)

A la fin du XXe siècle, on a assisté à l'émergence de structures continentales intermédiaires. L'exemple a été donné par les collègues africains, qui ont créé dès les années 1980 l'*Union mathématique africaine*. Sont ensuite apparues la *Société mathématique européenne* (SME), dont la gestation a été laborieuse — à l'image de celle de l'Union européenne — et qui regroupe depuis 1990 toutes les sociétés nationales de l'Europe géographique et d'Israël, et l'UMALCA, qui rassemble les mathématiciens d'Amérique du sud et des Caraïbes. Ces nouvelles structures sont nées de la volonté de renforcer des collaborations à l'échelle d'un sous-continent et, suivant les situations, de disposer d'un interlocuteur représentatif face à l'apparition d'un nouveau niveau politique (c'est le cas pour l'Europe) ou de contrôler l'aspiration des ressources par l'Amérique du nord (c'est le cas pour l'Amérique du sud) au lendemain de la douloureuse période des dictatures militaires.

Une présence de plus en plus large dans l'industrie et les services

Où sont employés les mathématiciens ? La grande nouveauté est que, de nos jours, des mathématiciens sont présents dans de nombreux secteurs de l'industrie et des services. Il n'y a cependant pas d'« industrie mathématique » comme il y a une industrie chimique ou une industrie pharmaceutique. En effet, les emplois confiés à des personnes à haute compétence mathématique portent souvent des dénominations variables, ce qui rend difficile le dénombrement des « mathématiciens industriels ». Une estimation récente laisse penser qu'ils sont près de 2000 à être employés de cette façon en France. Ce nombre est à comparer à celui de leur contrepartie académique (mathématiciens des universités, Grandes écoles et organismes de recherche divers), dont on estime l'effectif de façon beaucoup plus fiable à environ 4000. La ventilation de cette communauté académique entre organismes de recherche publics et enseignement supérieur (10 % contre 90 % environ) est un peu singulière : généralement, dans les autres disciplines scientifiques, un choix différent a été fait, puis-

qu'une proportion beaucoup plus importante consacre tout son temps à la recherche, sans tâches d'enseignement.

Quels sont les secteurs particulièrement intéressés à embaucher des mathématiciens ? Les banques et les assurances font un usage de plus en plus intensif de compétences mathématiques ; les produits qu'elles vendent reposent souvent sur une construction mathématique qui en est tout le fondement. Mais il en va de même d'un certain nombre d'entreprises de haute technologie dans lesquelles l'étude de systèmes complexes requiert une approche mathématique, que de puissants moyens de calcul fournis par les nouvelles générations d'ordinateurs peuvent rendre opératoire. Ces ouvertures nouvelles sont de nature à changer considérablement l'image des mathématiques auprès des étudiants. Cependant, elles n'ont pas encore été complètement assimilées par l'enseignement supérieur français ; le plus souvent, la raison en est l'inertie excessive du système éducatif, qui reste centré sur les formations aux professions académiques.

Les mathématiciens sont confrontés à une nouvelle donne

Ces nouveaux développements n'ont pas été sans avoir des répercussions sur la structuration des mathématiques, tant dans les établissements d'enseignement supérieur et de recherche qu'au niveau des publications. On a quelquefois présenté la situation ainsi créée comme une bataille entre « mathématiques pures » et « mathématiques appliquées ». Cette façon de voir les choses est injustifiée, pour au moins deux raisons. D'une part, les exemples de situations historiques où des mathématiques nouvelles ont été développées à partir de sollicitations extérieures abondent ; d'autre part, les nouveaux domaines à conquérir ne peuvent être abordés en déclarant *a priori* quelle partie des mathématiques sera la clef du problème posé. De nombreux rapprochements-surprises ont pu être constatés, qui prouvent que la dichotomie pure/appliquée est en fin de compte improductive. C'est dans le contexte de tension interne à la communauté mathématique qu'est née en France, en 1983, la *Société de mathématiques appliquées et industrielles* (SMAI). Vingt ans plus tard, les deux sociétés, SMF et SMAI, ont trouvé un mode de coopération efficace et mènent ensemble des actions d'intérêt commun. À elles deux, elles mobilisent plus de 3 000 personnes, dont l'appartenance va bien au-delà de la communauté académique pour la SMAI.

La nouveauté principale vient de la possibilité d'étudier de plus en plus de systèmes complexes grâce à l'usage de modèles de natures diverses. La modélisation est, aujourd'hui, une démarche à laquelle on recourt souvent. Ce nouvel engouement nécessite une réflexion plus approfondie sur les fondements, y compris philosophiques, de cette approche. L'une des capacités qu'il convient de développer est la confrontation du modèle à la réalité qu'il est censé représenter.

On peut néanmoins souligner deux tendances lourdes qui se nourrissent de ces nouveaux contacts des mathématiques avec un monde qui leur est extérieur : un regain d'importance donnée aux structures finies (structures mathématiques ne mettant en jeu qu'un nombre fini d'éléments) et la généralisation des approches stochastiques (faisant intervenir des processus aléatoires). Dans le deuxième domaine, la France a remarqua-



blement su prendre le virage, si l'on y compare la situation avec celle des pays de même niveau de développement, à l'exception peut-être d'une sous-représentation des statistiques et de l'analyse des données. En revanche, l'enseignement des mathématiques discrètes, c'est-à-dire portant sur les structures finies, y est toujours aussi discret : très peu de cursus d'enseignement supérieur offrent dans ce domaine une formation suffisamment complète.

Récemment, lors d'un colloque consacré à l'histoire de la géométrie dans la deuxième moitié du XXe siècle, Stephen Smale, un mathématicien américain qui fut l'un des pères de la topologie moderne et qui s'est par la suite intéressé de très près à l'analyse numérique, fit une remarque pertinente : aujourd'hui, l'extraordinaire croissance des mathématiques est aussi assurée par des personnes que les mathématiciens tendent à ne pas reconnaître comme faisant partie de leur communauté. Il est vrai que les statistiques, l'automatique, la recherche opérationnelle, la théorie du contrôle sont souvent peu représentées dans les départements de mathématiques des universités, alors que le cœur de toutes ces disciplines est vraiment mathématique. On pourrait en dire de même d'une bonne partie de l'informatique théorique : celle-ci entretient, avec les mathématiques, des liens organiques dont la profondeur et la force ne sont pas toujours reconnues par les mathématiciens eux-mêmes. Cette situation ouvre à la communauté des mathématiciens des possibilités de croissance considérable, pourvu qu'ils se montrent moins prompts à exclure ces activités nouvelles de leur champ. Avec plus de curiosité et d'ouverture, il y aura davantage de stimulations et de nouveaux champs d'action, pour le plus grand bien du développement des mathématiques elles-mêmes.

La mutation de la profession exige de nouveaux profils de formation

Une des premières choses à reconnaître concerne la pratique du métier de mathématicien requise par ces nouveaux contacts, pratique qui ne peut se limiter à prouver des théorèmes. On a aujourd'hui besoin qu'un nombre suffisant de mathématiciens aux profils très divers s'intéressent aux applications. Cela exige qu'ils apprennent à échanger avec des spécialistes d'autres disciplines, en offrant une écoute d'une qualité suffisante.

Dans diverses structures d'enseignement supérieur de par le monde, on constate déjà la mise en place de formations spécialisées, en mathématiques financières par exemple. D'autres créneaux, pour lesquels des débouchés importants hors du monde académique sont apparus, vont certainement voir le jour, à une échelle adaptée à ces débouchés ; c'est déjà le cas pour les formations d'actuaires, et l'on peut anticiper que des formations mixtes verront le jour à l'interface des mathématiques avec la biologie et la médecine par exemple.

Laisser proliférer des formations trop spécialisées serait une erreur, pour deux raisons : l'étroitesse des approches de ce genre d'une part, et le risque de coupure de la communauté mathématique qu'une telle pratique présenterait d'autre part. Pour que les étudiants perçoivent de manière plus naturelle les nouvelles orientations accessibles aux méthodes mathématiques, des modifications plus profondes des cursus de formation devront vraisemblablement être mises en



place. Il faut avoir l'ambition de créer une bonne fluidité entre le monde académique et le monde de l'industrie et des services ; c'est une condition pour que l'irrigation en bons problèmes, portant le plus souvent sur des champs nouveaux, se produise assez spontanément, et pour que ces problèmes soient traités avec le niveau de profondeur requis.

Jean-Pierre Bourguignon
CNRS-IHÉS (Institut des hautes études scientifiques, Bures-sur-Yvette) et École polytechnique, Palaiseau

Quelques références :

- B. Engquist et W. Schmid (eds.), *Mathematics unlimited — 2001 and beyond* (Springer-Verlag, 2001).
- C. Casacuberta, R. M. Miró-Roig, J. M. Ortega, et S. Xambó-Descamps (eds.), *Mathematical glimpses into the 21 st century, Round tables held at the 3rd european congress of mathematics* (Societe Catalana de Matemàtiques, Barcelona, 2001).

Comment devenir mathématicien ?



Maurice Mashaal

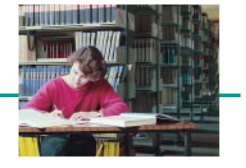
De longues années d'apprentissage et des talents évidents sont nécessaires pour qui veut faire de la recherche fondamentale en mathématiques. Mais les passionnés ont à leur disposition plusieurs filières de formation, avec des débouchés variés.

Au XVIIe siècle, un certain magistrat toulousain du nom de Pierre de Fermat (1601-1665) occupait ses heures de loisir à des recherches mathématiques et à entretenir une correspondance à leur sujet. Bien que ce ne fût pas sa profession, Fermat réalisa des découvertes mathématiques importantes. Il fut par exemple un pionnier de l'introduction des techniques algébriques en géométrie, et ses travaux en théorie des nombres l'ont rendu célèbre — notamment pour une conjecture qu'il formula et qui ne fut démontrée qu'en 1994 (celle-ci affirme que l'équation $x^n + y^n = z^n$ n'a pas de solutions x, y, z en nombres entiers positifs dès que l'entier fixé n est supérieur ou égal à 3). Fermat était, en fait, l'un des plus brillants mathématiciens de son siècle.



Un cours de mathématiques à l'université. (Cliché Institut de mathématiques-Université Bordeaux 1)

Cette époque où une personne douée pouvait faire des découvertes significatives en autodidacte, à ses heures perdues, est révolue. Certes, il arrive encore que des passionnés de mathématiques, dont ce n'est pas la profession, découvrent et prouvent ici ou là un nouveau théorème. Non seulement de tels cas sont rares, mais surtout les résultats obtenus portent généralement sur des questions



de détail, à la marge des grands courants de l'évolution des mathématiques.

Non, si quelqu'un aujourd'hui désire devenir un véritable acteur des mathématiques, il lui faut d'abord affronter de longues années d'études. Environ huit ans après le baccalauréat sont nécessaires afin d'assimiler les connaissances et les capacités essentielles, qui permettront à l'apprenti-mathématicien d'acquérir de l'autonomie et de commencer à produire à son tour des résultats mathématiques originaux.

L'itinéraire classique : DEUG, licence, maîtrise, DEA et thèse de doctorat

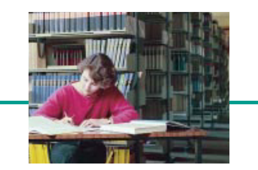
De longues études supérieures, d'accord, mais lesquelles ? La voie traditionnelle, en France, consiste à suivre un premier cycle universitaire de deux ans, puis un deuxième cycle de deux ans, et enfin un troisième cycle d'environ quatre ans.

Le premier cycle est l'objet du DEUG (Diplôme d'études universitaires générales). Pour les futurs mathématiciens, il s'agit généralement du DEUG scientifique mention « Mathématiques, informatique et application aux sciences » (MIAS), dont l'enseignement est centré sur les mathématiques, l'informatique et la physique ; ou du DEUG « Mathématiques appliquées et sciences sociales » (MASS), construit autour des mathématiques et de l'informatique d'une part, des sciences économiques ou humaines d'autre part.

La première année du deuxième cycle universitaire est consacrée par le diplôme de *licence*, la deuxième par le diplôme de *maîtrise*. Il peut s'agir d'une licence et d'une maîtrise de mathématiques pour qui se destine à la recherche fondamentale en mathématiques, ou d'un deuxième cycle MASS pour ceux qui s'intéressent aux mathématiques appliquées aux sciences économiques et sociales, ou encore d'une maîtrise d'ingénierie mathématique, orientée vers les applications industrielles, avec un accent sur l'analyse numérique, la modélisation, l'informatique, les probabilités et les statistiques.

Le troisième cycle commence par l'année du DEA (Diplôme d'études approfondies), dont il existe une grande variété (en mathématiques, il existe près d'une cinquantaine d'intitulés différents sur toute la France). Il peut s'agir de DEA encore généralistes, couvrant un spectre assez large des mathématiques, ou de DEA plus spécifiques, comme un DEA d'algorithmique ou un DEA de biomathématiques. Le choix du DEA est déterminant ; c'est généralement au cours de cette année que l'étudiant va entrer au contact de la recherche mathématique, qu'il va être confronté à des thèmes d'actualité, qu'il va devoir se plonger dans des articles de recherche publiés même très récemment.

Le DEA conditionne largement la suite, à savoir le doctorat qui se prépare généralement en trois ans. L'étudiant détermine son champ de recherche, se trouve alors un directeur de thèse et un laboratoire d'accueil, puis travaille sur le thème choisi en vue d'obtenir lui-même des résultats originaux, qui feront l'objet d'une ou plusieurs publications dans les revues professionnelles. Le diplôme de doctorat est décerné après rédaction et soutenance d'une thèse, en public, devant un jury composé de spécialistes.



Magistères et Grandes écoles, tremplins vers la recherche fondamentale

Licence, maîtrise, DEA, thèse : tel est, en résumé, le parcours d'études conventionnel en France pour devenir chercheur en mathématiques ; à cela s'ajoutent souvent une ou plusieurs années de recherches post-doctorales, rémunérées à l'aide de bourses ou de contrats à durée déterminée et parfois effectuées à l'étranger, avant que le jeune mathématicien ne réussisse à décrocher un poste stable de chercheur ou d'enseignant-chercheur. Ce modèle est *grosso modo* le même dans la plupart des pays. C'est le type d'itinéraire qu'ont suivi des personnes comme Andrew Wiles, le mathématicien britannique qui est venu à bout, en 1994, de la fameuse conjecture de Fermat.

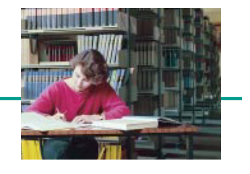
En fait, le parcours que l'on vient de décrire comporte plusieurs variantes ou exceptions importantes. Tout d'abord, en France, les Grandes écoles comme les Écoles normales supérieures et l'École polytechnique ont tendance, en mathématiques, à drainer les étudiants les plus brillants. Pour présenter les concours d'entrée à ces établissements très sélectifs, les candidats suivent non pas un DEUG, mais deux (voire trois) années de « classes préparatoires » en lycée, caractérisées par une préparation intensive et un investissement personnel plus important. Après le concours d'entrée, les élèves normaliens s'intègrent aux deuxième puis troisième cycles universitaires ; les élèves polytechniciens, eux, suivent deux années de formation à l'École polytechnique même, puis rejoignent s'ils le souhaitent la filière universitaire au niveau du DEA. Le passage par une École normale supérieure ou par l'École polytechnique n'est pas obligatoire pour qui veut devenir mathématicien ; cependant, il faut le reconnaître, la plupart des postes de chercheurs en mathématiques fondamentales sont occupés, en France, par d'anciens élèves normaliens ou polytechniciens.

Par ailleurs, plusieurs universités proposent des *magistères*, formations d'excellence en trois ans qui intègrent la licence, la maîtrise et un DEA, dans lesquelles les étudiants (en bonne partie des normaliens) sont sélectionnés sur dossier après un DEUG ou une classe préparatoire. Les futurs chercheurs ont plutôt intérêt à suivre un magistère, plutôt que le cursus habituel.

Signalons également qu'il existe de multiples passerelles entre les écoles d'ingénieurs et l'université. Ainsi, les élèves des écoles d'ingénieurs peuvent, selon leurs centres d'intérêt et leur niveau, rejoindre la filière universitaire, pour un DEA ou pour une thèse de doctorat. Inversement, des étudiants d'université peuvent dès la fin du DEUG et dans certaines conditions intégrer une école d'ingénieurs, voire, ultérieurement, une Grande école.

Le profil d'ingénieur : des études moins longues, mais aussi moins orientées vers la recherche

Disons quelques mots des écoles d'ingénieurs, qui recrutent généralement leurs élèves sur concours, après les classes préparatoires. Bien qu'il s'agisse *a priori* de former des ingénieurs et non des chercheurs, l'enseignement en mathématiques y est souvent de bon niveau. Certaines de ces écoles conviennent particulièrement à ceux qui souhaitent allier les mathématiques et un domaine d'ingénierie



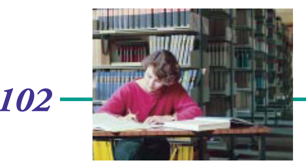


En mathématiques, plus encore que dans les autres disciplines scientifiques, la bibliothèque est un outil essentiel — pour les étudiants comme pour les chercheurs. (Cliché Institut de mathématiques-Université Bordeaux 1)

ou de technologie, comme la mécanique, l'acoustique, l'informatique ou autre. Il existe aussi des écoles spécialisées, telles que l'ENSAE (École nationale de la statistique et de l'administration économique) ou l'ENSAI (École nationale de la statistique et de l'analyse de l'information) qui forment des statisticiens, l'EURIA qui forme des actuaires, etc.

La formation d'ingénieur permet, en quatre ou cinq années d'études supérieures, une entrée assez rapide dans la vie active. Évidemment, la nature de l'activité exercée par un ingénieur-mathématicien travaillant dans une entreprise ne sera pas la même que celle d'un chercheur travaillant dans un laboratoire de recherche : elle consistera davantage à appliquer des mathématiques déjà connues à des problèmes concrets qu'à créer des mathématiques nouvelles. Cependant, entre les deux types d'activité, on peut rencontrer tous les intermédiaires, en fonction de l'entreprise, de l'organisme ou du laboratoire, et en fonction de la personne et de sa formation. Par exemple, un ingénieur ayant été formé à la recherche au travers d'une thèse de doctorat et travaillant dans une grande entreprise de haute technologie peut être amené à effectuer des recherches de nature fondamentale.

Enfin, il faut savoir que des formations de type ingénieur sont également dispensées par les universités, à travers les Instituts universitaires professionnalisés (IUP) ou les maîtrises à finalité professionnelle comme les MIAGE (maîtrise en méthodes informatiques appliquées à la gestion des entreprises) et les MST (maîtrise de sciences et techniques). Comme les écoles d'ingénieurs, ces formations de type bac + 4 ne sont pas particulièrement ou exclusivement centrées sur les mathématiques. Mais un DESS (diplôme d'études supérieures spécialisées), sorte de DEA à finalité professionnelle, peut compléter une telle formation et lui donner une orientation mathématique plus marquée. Il existe ainsi des DESS de « Calcul scientifique et informatique », d'« Ingénierie mathématique », de « Mathématiques, informatique et sécurité de l'information », de « Modélisation stochastique et recherche opérationnelle », etc. : le choix est vaste !



L'interdisciplinarité, une clef pour l'avenir

Beaucoup sont conscients de la nécessité d'une ouverture plus grande des mathématiques vers les autres disciplines. Les mathématiques de pointe se révèlent utiles et nécessaires dans des domaines de plus en plus nombreux ; inversement, les problèmes concrets posés dans ces domaines peuvent inspirer des recherches fondamentales fructueuses, qui font progresser la science mathématique elle-même. Au sein des institutions d'enseignement et de recherche, apparaît la volonté politique de développer l'interdisciplinarité, mais elle a encore du mal à se traduire dans les faits.

Un des principaux terrains d'action est l'enseignement supérieur. Si, au niveau des DEA et des DESS de mathématiques, on remarque une certaine ouverture vers d'autres domaines, la situation en deuxième cycle universitaire (licence et maîtrise) semble plus préoccupante : « les mathématiques y sont enseignées de façon presque totalement monolithique ; il faut repenser les programmes, qui ont très peu évolué au cours des dernières décennies », *affirme Jean-Pierre Bourguignon, directeur de l'Institut des hautes études scientifiques (IHES).* « Par exemple, l'interface entre mathématiques et biologie ou médecine est quasiment inexistante, et il en est de même des mathématiques discrètes ». *On peut tout de même noter quelques évolutions, comme l'instauration au concours de l'agrégation d'une épreuve de modélisation.*

Un autre terrain d'action vers l'interdisciplinarité concerne les recrutements de chercheurs et d'enseignants-chercheurs, ainsi que l'avancement de leurs carrières. Comme le souligne Jean-Marc Deshouillers, directeur pour les mathématiques à la Mission scientifique universitaire (Ministère de la Recherche), « on peut favoriser les échanges interdisciplinaires à travers les commissions de recrutement », *pour que par exemple des spécialistes de statistique soient recrutés dans des laboratoires de biologie. On peut aussi créer de nouveaux laboratoires consacrés à des thèmes pluridisciplinaires, ou tenter de modifier l'orientation de laboratoires déjà existants, à travers leur évaluation. C'est ce que font déjà des organismes comme le CNRS ou le Ministère de la Recherche. Mais, sur le chemin de l'interdisciplinarité, les difficultés sont nombreuses : il faut rompre avec certaines habitudes, contourner des obstacles administratifs ou statutaires, surmonter les incompréhensions entre chercheurs de disciplines différentes, investir en hommes et en argent, etc. Les choses en sont encore à leurs débuts.* « La compétition et la spécialisation scientifiques, le système d'évaluation et de recrutement, ont trop souvent tendance à favoriser les profils conventionnels et peu mobiles », *dit Christian Peskine, directeur scientifique adjoint pour les mathématiques au CNRS ; le système ne suscite pas assez l'émergence de personnes ayant une formation originale, ayant envie de prendre des risques (scientifiques…) dans des domaines nouveaux. Mais ceux qui tiennent déjà un rôle et une place dans les thèmes interdisciplinaires pourraient avoir un effet d'entraînement et encourager d'autres collègues ou étudiants à les imiter.*

Des débouchés d'autant plus nombreux que la formation laisse de la place à d'autres disciplines

Les débouchés qui s'offrent aux diplômés en mathématiques ? Pour ceux qui sont allés jusqu'au doctorat et au-delà, les voies naturelles sont la recherche et l'enseignement supérieur : des organismes de recherche publique comme le CNRS, l'INRIA, le CEA, l'ONERA, etc., mais aussi de grandes sociétés comme la RATP ou EDF-GDF, recrutent des chercheurs, et les universités recrutent des enseignants-chercheurs ; de même, les Grandes écoles ou les écoles d'ingénieurs recrutent des enseignants et, dans les cas où elles possèdent des laboratoires de recherche, des chercheurs. Cependant, le nombre de postes offerts par la recherche et l'enseignement supérieur ne sont pas très nombreux, et cette voie est donc très sélective. À titre d'illustration, le CNRS (Centre national de recherche scientifique) recrute une quinzaine de jeunes « chargés de recherche » mathématiciens par an (20 en 1995, 13 en 1997), les universités une centaine de « maîtres de conférences » (116 en 1995, 111 en 1997) ; ces chiffres sont à comparer au nombre de diplômes de doctorat délivrés en mathématiques, qui tourne autour de 350-400 annuellement (en France).

Les entreprises privées, quant à elles, embauchent traditionnellement des ingénieurs ; peu de mathématiciens (au sens de chercheurs) y trouvent place. Cependant, la nécessité de recherches mathématiques pointues se fait sentir dans un nombre croissant de domaines (finance, assurance, informatique, télécommunications numériques, robotique, industrie aéronautique et spatiale, recherche pétrolière, etc.). Aussi, la présence de mathématiciens dans les entreprises est appelée à augmenter ; et une telle intégration se fera d'autant plus aisément que la formation du mathématicien aura comporté des ouvertures vers d'autres disciplines (voir l'encadré).

À un niveau moins élevé que le doctorat, les études mathématiques offrent des débouchés plus nombreux, mais les métiers correspondants s'éloignent de celui de mathématicien à proprement parler. Une voie numériquement importante est l'enseignement secondaire : le métier d'enseignant en lycée est accessible après une licence ou une maîtrise, puis une année de préparation au concours du CAPES (après licence) ou de l'agrégation (après maîtrise). Mais il y a une kyrielle de possibilités d'emplois faisant appel à des compétences mathématiques, dans les banques, dans les assurances, en informatique, dans les services de « recherche et développement » des entreprises, etc. À condition que les études aient inclus une ou plusieurs spécialités en plus des mathématiques, le risque de se retrouver sans travail est bien faible.

Maurice Mashaal
journaliste scientifique

Quelques références :

- *Infosup n° 189*, janvier-février 2001 (Dossier de l'ONISEP sur les études universitaires de mathématiques et leurs débouchés).
- Site Internet de l'ONISEP (Office national d'information sur les enseignements et les professions) : http://www.onisep.fr.
- *Mathématiques à venir - où en est-on à la veille de l'an 2000 ?* supplément au n° 75 de la *Gazette des mathématiciens*, publié par la SMF et la SMAI (1997).

Sommaire

